THE PAYPERS

Web Fraud Prevention, Identity Verification & Authentication Guide 2018-2019

LATEST INSIGHTS INTO DIGITAL ONBOARDING AND FRAUD MITIGATION FOR BANKS, MERCHANTS AND PSPS

Key Media Partners

mpe Merchant Payments Ecosystem

Endorsement Partners

MRC Building Better Commerce Fraud & Payments Professionals

HOLLAND FINTECH

THE PAYPERS

Web Fraud Prevention, Identity Verification & Authentication Guide 2018-2019

LATEST INSIGHTS INTO DIGITAL ONBOARDING AND FRAUD MITIGATION FOR BANKS, MERCHANTS AND PSPS

Contact us

For inquiries on editorial opportunities please contact:

Email: **editor@thepaypers.com**

To subscribe to our newsletters, click **here**

For general advertising information, contact:

Mihaela Mihaila

Email: **mihaela@thepaypers.com**

RELEASE VERSION 1.0
DECEMBER 2018

TEL: +31 20 893 4315
FAX: +31 20 658 0671
MAIL: EDITOR@THEPAYPERS.COM

Editor's letter

Customer experience and the **conflict between offering a frictionless customer service to good clients while managing risk and blocking the bad guys** are some themes that are emerging from acquirers, card schemes, regulators, service providers, merchants, as well as auditors and journalists alike.

Identifying fraudulent behaviour without rejecting or offending good customers is key because a blocked good customer will not return, and as the market is so competitive, they can go everywhere. Moreover, *automation technologies based on machine learning and artificial intelligence are gaining prominence* in this conversation. But, as always, some challenges in addressing these themes, security-wise, still remain.

The Web Fraud Prevention, Identity Verification & Authentication Guide 2018-2019

To respond to some of these challenges, **we have released our 7th edition of the Web Fraud Prevention, Identity Verification & Authentication Guide** to provide payment and fraud and risk management professionals with a series of insightful perspectives from industry associations and leading market players on key aspects of the global digital identity, transactional and web fraud detection space.

The guide is structured in three parts; the first part focuses on presenting the industry, with its most acute problems, but also shares some best practices from industry leading players on how to tackle them. With the advent of digitalisation and the use of smartphones, **business and fraud coexist globally, both seen as profitable activities**, involving large masses of customers. The surge in demand for many goods and services has enabled **not only businesses' profits to soar but also fraudsters to capitalize on this growth**. Bad actors are tricking retailers/merchants/banks by hiding beneath large transaction volumes and exploiting the fact that many products and services providers are willing to accept a greater degree of risk in order to approve more orders.

Key challenges for businesses

One of the biggest **challenges in the fraud detection space** for retailers/merchants is that **for consumers, a transaction needs to happen in the blink of an eye**, and therefore fraud controls should be invisible for them.

However, **fraud attacks are becoming more sophisticated**, with fraudsters having access to the latest technology and sophisticated tools. Therefore, **what is really needed? A fraud management solution can track the customer's behavioural patterns** (behavioural profiling) and **instantly detect and report any signs of fraud, triggering a step up authentication to mitigate the potential risk** (risk-based authentication).

Similarly, **when it comes to financial institutions (FIs)**, FIs are under intense competitive pressure to **make the banking experience easier and frictionless** (while regulators in Europe appear to be taking the industry in a different direction, thanks to the second Payment Services Directive's requirement for Strong Customer Authentication).

The faceless nature of the online and mobile channels makes authentication hard, however the large amounts of data that have been breached in recent years combined with fraudsters' use of phishing, social engineering, and malware make authentication much more difficult. As a result, **some of the top threats for 2018 in ecommerce and banking are account takeover and new account applications, according to Aite**.

For Europe especially, but also for the US, Canada and Australia, in 2018, financial discussions revolved around **Open Banking initiatives**. The concept of open banking **promises users greater control over their financial data**; however, it is not without risks, and **its success is tied to consumer confidence when it comes to the security and privacy of their information**.

At the moment, **businesses have become incredibly dependent on a network of systems to manage, store, and transmit information** such as financial accounts, personally identifiable information, intellectual property, transaction records etc. Within this web, authentication, validation and verification have turned out to be central to the ability of these businesses to effectively secure access to consumer-facing digital channels and the systems that underpin their operations. →

The right tools for fighting fraud

The second part of our **Web Fraud Prevention, Identity Verification & Authentication Guide 2018-2019** focuses on mapping the key players in the **fraud detection, identity verification and online authentication space**. The chapter aims to create an accurate picture of **what the fraud detection, identity verification and online authentication offerings looks like**, and it **displays the key players of the industry together with their main capabilities**. Depicting the most important features of each company is part of our goal of helping merchants, banks, fintechs and payment service providers to grasp the current market opportunities and to use them according to their own needs.

The whole range of capabilities is designed to address the pain points that organizations in the payments space are struggling to remove. To do so, **security and risk management leaders** involved in online fraud detection **have started using machine-learning analytics, cloud-based deployment options, artificial intelligence, behavioural analytics, and massive global data networks**.

Such technologies generate real-time insights into the nuanced patterns of fraud to enable businesses to spot and fight fraud. These patterns are based on geography, industry, time of day, time of year, and over 15,000 other signals. Fraud management specialists/vendors have developed networks that analyse millions of transactions in real time across billions of devices.

Finally, the third part of our **Web Fraud Prevention** guide, the **Company Profiles section**, offers insights into the capabilities fraud prevention companies offer businesses in order to spot fraudulent attacks, stop them and prevent them from happening.

Obviously, we would like to **express our appreciation** to the **Merchant Risk Council** and **Holland FinTech** – our endorsement partners who have constantly supported us – and also to **our thought leaders, participating organisations** and **top industry players that contributed to this edition**, enriching it with valuable insights and, thus, joining us in our constant endeavour to depict an insightful picture of the industry.

Conclusion

Businesses may think they understand fraud, but the reality is far more complex, and this lack of insight **could lead to guessing, incorrect conclusions, and bad decisions. Premises** such as the **fraudsters as geeky guys, conducting their activities at night in their basements**, and **living somewhere in Eastern Europe**, or that **ATOs are relatively low profile events** could shape businesses' fraud-fighting operations from top to bottom. Moreover, these assumptions help determine how analysts set up rules, how many people the fraud team hires and staffs on a given day, and so on.

Therefore, **security and risk management leaders responsible for fraud prevention and payment security should align with cross-organisational groups** (security, identity and access management, credit/underwriting) to **detect high-risk or anomalous activity** and identity, and **tap into technologies that enable fighting against these threats**. And if we consider the large amounts of harvested data, **the capability of analysing and connecting data across channels is vital for strong defence**.

Enjoy your reading!

Mirela Ciobanu
Senior Editor, The Paypers

Table of contents

Table of contents

Table of contents

Fraud Management – Trends and Developments

Overview on the Innovation Taking Place in the Fraud Management Space – Machine Learning and Artificial Intelligence

The Rise of Machine Learning/ Artificial Intelligence in Fraud Detection

Mirela Ciobanu | *Senior Editor* | The Paypers

The lines are blurring between man and machine. As advances in AI, smart tech, and machine learning turn science fiction into fact, a future once fantastical draws near now. How will the payments industry harness these mind-blowing opportunities?

Artificial intelligence and machine learning have a wide array of applications, from improving customer experience to enabling businesses to fight fraud, from driving the creation of personalised shopping/user experiences by analysing multiple data points to enabling businesses to stay compliant with the ever changing regulation landscape – KYC, AML. Moreover, these emerging technologies have also been applied in medicine; popular AI solutions such as IBM's Watson are actively used in multiple cancer research hospitals, and they operate as a doctor's assistant.

However, in this subchapter we will mostly focus on the ways in which these technologies can help fight fraud, manage and mitigate risk, and enable companies to stay compliant with AML laws and fight transaction laundering.

Artificial intelligence

Artificial intelligence (AI), sometimes called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans and other animals. AI augments human intelligence and should provide explanations to avoid erroneous interpretations, and its value should be considered in context, as definitive answers do not exist, according to Pedro Bizarro, Chief Science Officer, Feedzai.

AI design principles should be transparency, controllability, and automation. Moreover, data provenance is a crucial feature, as the user needs to keep track of data in order to be able to reconstruct it, and models should learn from real data, and be able to re-learn, while not being influenced/based on previous models. Most importantly, we must create the means of developing this tool in order for it to be human-enabled and human-centric.

According to Forbes, AI needs to be 'Explainable' and 'Understandable'. **Explainable AI** is the domain of data scientists and AI engineers, the individuals who create and code artificial intelligence algorithms. These specialists aim to develop new algorithms that explain intermediate outcomes or provide reasoning for their solutions.

Understandable AI combines not only the technical expertise of engineers with the design usability knowledge of UI/UX experts, but also the people-centric design of product developers. **Explainable AI** is different from **understandable AI**. Since AI-driven solutions need to be developed with 'user-first' principles in mind, **understandable AI** has become the domain of UI/UX designers and product developers, in collaboration with AI engineers and data scientists.

Critical to the **understandable AI** *process are the integration of non-data scientists to the development and design of AI products and enabling people to be a part of the decision-making process in an AI-driven enterprise*. ➔

The Rise of Machine Learning/ Artificial Intelligence in Fraud Detection

To begin the journey towards a **truly human-machine collaborative model** that creates understandable AI outcomes, **leaders, governance bodies, and companies must**:

- **develop intuitive user interfaces** – by using voice recognition and natural language processing, the technology industry is currently developing AI user interfaces that enable people to interact with intelligent machines simply by talking to them. By encouraging the development of these tools, the democratisation of AI technologies is encouraged;
- **create ethical principles for AI** – all major stakeholders in the future of AI need to work together to build principles that embed understandability into technology development;
- **apply design principles** – enterprises should use design-led thinking to examine core ethical questions in context. In addition, they are advised to build a set of value-driven requirements under which the AI will be deployed – including where explanations for decisions are expected;
- **monitor and audit** – the AI solutions used at the enterprise level need to be continually improved through value-driven metrics such as algorithmic accountability, bias, and cybersecurity.

When it comes to financial services, artificial intelligence can be applied to specific areas such as financial crime prevention, regulatory compliance, and payments. Successful AI projects rely on the deep amounts of research and work that expertise developers put in, and the application to specific business problems, which can be used in multiple different contexts. A critical element of AI systems is the data on which they are trained – it's that combination of innovative AI capabilities and deep domain expertise.

A fundamental concept of AI is machine learning – that is why sometimes these two technologies go intertwined.

Machine learning – an approach to fraud detection and protection

Machine learning, a form of artificial intelligence, combines data, context, and feature engineering to allow organisations evaluate the risk of a particular digital interaction or purchase.

Machine learning is being used at many levels in the online fraud detection market. Some solutions are designed to run alongside existing capabilities, taking in structured and unstructured data to identify anomalies, while others are designed to provide a score and information codes that can be used by a real-time policy and decision engine.

A machine learning solution needs access to a big store of historical data to train its models and increase the probability that it will uncover patterns of new suspicious activity. This technology has the potential to fight card-not-present fraud, chargebacks, account takeover, transaction laundering, and more. Also, machine learning is implemented in solutions such as device assessment, passive behavioural biometrics, bot detection, phone printing, and voice biometrics. →

The Rise of Machine Learning/ Artificial Intelligence in Fraud Detection

With the waves of new and evolving fraud, Gartner has observed the increasing need of financial institutions and enterprise-scale merchants for rapid and complex risk decisions, and businesses are turning to machine learning to gain the ability to make rapid and effective risk decisions. However, with the increased number of machine-learning systems, clients are demanding explanations, as well as decisions, with the aim of:

- controlling the machine – a model that explains its logic empowers security managers to adapt the model to evolving fraud patterns with more speed and accuracy;
- auditing the machine – financial institutions and large merchants operate in highly regulated environments. These organisations need to provide trails of explanations for compliance, to demonstrate that the basis for their decisions is lawful and ethical;
- trusting the machine – a system is only as powerful as the decisions we entrust it to make. How can we trust that the machine is finding the delicate balance between good risk management and good CX?

To achieve these goals, Gartner suggests that businesses should ensure that each model they develop incorporates a capability to explain and, moreover, has a loop that provides feedback on the quality of the explanation. The second method is to develop two systems – one that makes decisions and another that takes the input from the first system and generates an explanation.

Here are some types of machine learning that can be deployed:

- **Deep Learning** – is a class of machine learning algorithms that use a cascade of multiple layers of nonlinear processing units for feature extraction and transformation. Each successive layer uses the output from the previous layer as input. These algorithms learn in supervised (eg classification) and/or unsupervised (eg pattern analysis) manners and understand multiple levels of representations that correspond to different levels of abstraction; the levels form a hierarchy of concepts.

– **Ensemble Learning** – ensemble methods use multiple learning algorithms to obtain better predictive performance than could be obtained from any of the constituent learning algorithms alone.

– **Unsupervised Learning** – does not require outcomes, so it can learn without waiting for the completion of a three-month chargeback reporting cycle, for example. This type of learning often relies on clustering, peer group analysis, breakpoint analysis, or a combination of these. This enables fraud prevention solutions to detect patterns and anomalies rapidly within extremely large sets of data.

- **Supervised Learning** – uses outcome-labelled training data sets to learn. Models include neural networks, Bayesian classifiers, regression, decision trees, or an ensemble combination. Massive amounts of data run through defined models to assess risk outcomes.

The power of supervised and unsupervised machine learning

There are two approaches that are used mostly by fraud prevention vendors – supervised and unsupervised learning, the former approach being the most common and widespread. ➔

The Rise of Machine Learning/ Artificial Intelligence in Fraud Detection

Maxpay explains briefly how these systems interact to identify anomalies (outliers). With the supervised approach, in the beginning, a risk analyst creates a machine learning model based upon historical data. Afterwards, with new transaction data, the algorithm creates potentially right baskets: fraud and not fraud. After that, the system collects external signals such as fraud alerts, chargebacks, complaints etc. Based on that information, the algorithm starts looking for new unrecorded dependencies. Finally, the model starts retraining. Consequently, all the risk analysts are one step behind the game, thus the cycle continues, and in time new techniques emerge.

Otherwise, unsupervised learning is regarded as an alternative to supervised learning. These algorithms infer patterns from a dataset without reference to known or labelled outcomes. Unsupervised learning allows risk analysts to approach problems with no exact idea about what the result will look like. One can derive structure from data where they don't necessarily know the effect of the variables. With unsupervised learning, there is no feedback based on the prediction results. But it can divide data on the basis of anomalous behaviour and, afterwards, risk analysts can apply well-known supervised approaches to this data.

Therefore, unsupervised machine learning is more applicable to real-world problems and can help solve them when risk managers are one step behind the fraudsters.

As fraud prevention services use both rule-based and machine learning approaches, including unsupervised techniques, we should also consider that there is a significant difference between fraud detection systems that directly use machine-learning systems and those that are essentially static, rule-based systems. Characteristics of the former type include flexibility in response to new fraud attack patterns. The latter type benefits from keeping a human element in the change control process, which makes it more resistant to skilfully crafted attacks that try to poison the model.

Some banks, merchants, retailers have traditionally relied upon rules-based fraud detection systems in order to counter threats, such as leveraging weak points through coordinated attacks, but fraud advancements have outpaced the capabilities of these systems.

According to Feedzai, rules-based systems tend to be either too broad or too narrow in scope to adequately address fraud attack vectors, requiring financial institutions to combine multiple solutions into a single system to cover their bases.

Surely, machine learning does not replace rules completely, but it complements them to expand the capabilities of the risk management platform. Thus, when applied to large datasets, like those found in account opening analyses, these algorithms can pinpoint surprising and unintuitive fraud signals.

Computop

Machine Learning Against Online Fraud: The Advantage of a Risk-Based Approach

About Ralf Gladis: Ralf Gladis is the Co-Founder and CEO of the international payment service provider Computop – the payment people. In addition, Ralf acts as non-executive Director at Computop, Inc in New York. He is also responsible for the international expansion and strategic planning at Computop.

Ralf Gladis | *Co-Founder and CEO* | Computop

The increasing popularity of online shopping is creating new security risks in the transaction process. Data theft and payment fraud are issues that consumers and merchants alike fear. If we look at the current status of online fraud, we see that data breaches still represent a prevalent issue. Moreover, according to a research by the Identity Theft Resource Center and CyberScout, 791 data leaks were reported from large companies in the US **from January to June** 2017, with criminals stealing credit card information amongst other things. This represents an increase of 29% over the first half of 2016 and exceeded the 781 cases reported for the full year 2015 in just six months. Other studies confirm the trend: according to information service provider Experian, the number of data leaks in ecommerce **increased by 56% in 2017** compared to 2016.

Risk-based instead of rule-based

In the fight against fraud, payment service providers (PSPs) must have better tools at their disposal than ever before. Rule-based fraud prevention is replaced by risk-based fraud prevention. The difference: previous procedures allowed the risk assessment to be based on certain rules according to which a transaction was approved or rejected. The criteria were, for example, in which country the buyer uses a credit card, whether the device with which he pays online is unknown to the system, whether he uses the card several times at short intervals, and whether he exceeds a certain amount of money when paying. In practice, many other rules apply but, despite their complexity, they do not protect against fraud as effectively as the machine learning method does.

The new generation of risk management that has been used at Computop since the end of October 2018 is not only more flexible than before, but also more secure and efficient. The new Fraud Score Engine uses machine learning to automatically optimise fraud prevention and it eliminates the need for manual intervention. The algorithm behind the risk cost calculation learns with each transaction and improves the accuracy of the risk assessment accordingly. If buyer behaviour changes and new fraud scenarios emerge, it adapts. A concrete example illustrates this method:

Previously, the retailer made a yes/no decision in which various factors were queried, for example: 'If a transaction exceeds the amount X and is made in country Y, it is rejected.' On the other hand, an intelligent fraud scoring engine calculates probabilities: 'What proportion of all fraud cases recorded to date deal with amounts greater than EUR 500, and what percentage of successful, clean payments is greater than EUR 500?' This results in a data record that the system uses to calculate the probability of fraud. This method is much more accurate than the rule-based approach and can be applied to all parameters (payment location, device used, etc) that also use rule-based fraud prevention. The accuracy of the calculation improves with every payment transaction because, based on the empirical values from past transactions, the precision of the probability calculation for each individual parameter increases, thus the quality of the overall statement increases as well. Essentially, this is the greatest benefit of risk-based fraud prevention. ➔

Adaptable, fast and flexible

Combined with all the risk factors taken into account – such as transaction duration, correspondence between invoice and delivery address, use of an anonymisation service, and many more –, the engine calculates a score value within fractions of a second, which represents the basis for the decision, as to whether the transaction should be submitted to the card-issuing bank for protection via 3-D Secure.

If the risk factors regarding fraud represent less than a certain value, the system does not perform an additional query. In the case of a medium value, the bank either uses its own checking system to relieve the customer of entering a password or it requests the password directly. If the 3-D Secure procedure is used, the bank also takes over the liability risk from the merchant. If the score is clearly within the red range, the transaction is rejected directly.

The risk-based method fundamentally changes fraud prevention. Until now, rule creation was a manual process based on individual traders. The automation now increases flexibility and it is able to drive double-track. On the one hand, this approach assesses the risk-based on trader-specific transaction characteristics, and on the other hand, it uses the entirety of all anonymous transactions of the PSP for forecasts.

Therefore, each transaction is protected the best possible way, on the basis of the past, and subsequently contributes to further optimisation. In principle, PSPs include both successful transactions and chargebacks from the acquirer's settlement files in their risk analysis. Machine learning enables the scoring engine to move away from the purely manual adaptation to new threats, that has been adopted, so far, by organisations. This was time-consuming, inaccurate, and inflexible.

With machine learning, the reaction speed to fraudulent actions increases, as the retailer can rely not only on his own transaction data but also on risk assessments from Computop's past payment transactions – thus, on a significantly higher overall population. The combination of machine learning and rule-based risk prevention offers the best possible protection, with experienced experts monitoring the process and providing the artificial intelligence with the context it needs, to develop further and work with the right assumptions.

computop
the payment people

About Computop: Computop offers local and innovative omnichannel solutions for payment processing and fraud prevention around the world. For ecommerce, at POS and on mobile devices, retailers and service providers can choose from over 250 payment methods. Computop, a global player with locations in Germany, Canada, the UK and the USA processes transactions for more than 15,000 retailers annually, with a combined value of USD 31 billion.

www.computop.com

Click here for the company profile

CyberSource

Why Implement a Fraud Management Solution that Combines Machine Learning with Rules?

About Mark W. Hall: Mark is a seasoned entrepreneurial leader who is passionate about crafting multi-channel marketing programmes that communicate differentiation and clarity in the Enterprise B2B space. At CyberSource, Mark heads global cross-functional marketing, positioning, and messaging for the company's fraud solutions.

Mark W. Hall | *Sr. Director Global Solutions Marketing, Fraud Management* | CyberSource

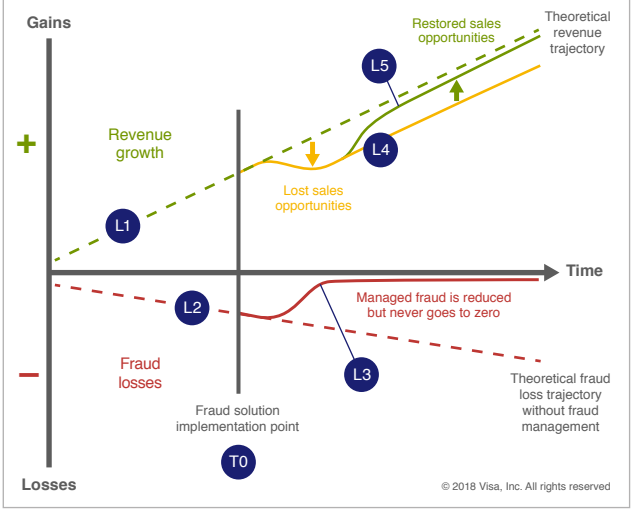
According to artificial intelligence (AI) pioneer Arthur Samuel, machine learning is a 'field of study that gives computers the ability to learn without being explicitly programmed.' For fraud management, this means that machine learning can detect subtle emerging fraud patterns that are impossible to see on a human level. Virtually, all fraud management systems today use some form of machine learning, so what sets CyberSource Decision Manager apart?

Importance of data: Decision Manager has had machine learning from the beginning. Decision Manager is the only machine learning fraud solution that draws insights from Visa and CyberSource's 68B+ annual transactions processed from around the globe. These transactions come from tens of thousands of merchants across a wide variety of industries and specialities. With this depth and breadth of data, it's like having more high-quality neurons in the machine learning 'brain.' It just makes sense that better data leads to better fraud detection decisions.

Why rules are needed: Another very important distinction with Decision Manager is the inclusion of powerful rules, which adds a level of precision control for Risk Analysts. But why are rules important? Let's explore a theoretical example of what can happen without rules in the following diagram.

Line L1 shows revenue growth before applying a fraud prevention tool. In the diagram, line L1 represents a theoretical revenue growth trajectory.

Why implement a fraud management solution that combines machine learning with rules?



Line L2 shows fraudulent activity as a percentage of revenue. As revenues grow, if fraud losses are left unchecked, they too would continue to grow as a percentage of revenues, as shown on line L2.

Line T0 represents the point in time when an organisation implements a fraud management solution. Once a business realises they have significant fraud losses, they will institute a fraud management system as shown at time T0.

Line L3 shows the reduced level of fraud by using a fraud management programme. As the fraud management system starts learning from that business' transaction data, the fraud loss level should gradually reduce as shown on the red line L3. →

It is virtually impossible to prevent all fraud; however, through active fraud management, the fraud percentage can get very low.

Line L4 represents the reduced level of revenue due to a poor customer experience while managing fraud. False positives can lead to lost revenues, as shown on the yellow line L4, not only due to the loss of the immediate sale, but even more by potentially losing a customer forever due of the rejected transaction. This has the impact of reducing revenue growth not only by interfering with business one transaction at a time, but tarnishing the experience for a legitimate buyer and compromising the lifetime value of customers.

Line L5 shows what active fraud management can do to restore revenues closer to the theoretical level. By combining rules with good manual review practices, many businesses may actually see an increase in revenue that comes very close to their theoretical revenue trajectory, as seen in the green line L5. Decision Manager's rules can be configured to activate at a specific time of day or date ranges, which can accommodate a variety of cyclic, seasonal, and periodic sales promotions – helping maximize acceptance rates and revenues.

Rules provide customised control: By instituting rules, a risk analyst can inject human intelligence and set common-sense parameters for their specific business. For instance, if the item being sold is a low priced digital good, like a picture or a song, the risk analyst might have a higher tolerance for the fraud risk score because there is no cost of goods. This is much different than an online retailer of big-ticket luxury items where the cost of goods is high – and there's an open market for fraudsters to easily turn those goods into cash. Obviously, in the latter case, the risk analyst will want to send questionable transactions to manual review prior to shipment.

The best of both worlds: Decision Manager employs machine learning that operates on insights from 68B+ global Visa and CyberSource processed transactions, enabling fast detection of emerging fraud patterns, while at the same time offering powerful rules that enable the injection of human ingenuity. Machine learning, combined with rules, provides an excellent fraud management solution.

Kount

Brick and Mortar Navigates Digital Transformation

About Don Bush: Don is the Vice President of Marketing at Kount. Prior to joining Kount, Don was the Director of Marketing at Cradlepoint, a leading manufacturer of wireless routing solutions in the mobile broadband industry. Don has worked in several management roles within the technology segment for over 20 years with both hardware/software manufacturers and as a partner in two top technology-marketing agencies.

Don Bush | *Vice President of Marketing* | Kount

Traditional brick and mortar merchants are expanding beyond their four walls to engage with customers through mobile apps, kiosks, desktops, and other digital platforms. At the forefront of this digital transformation is the introduction and branding of trademarked native mobile apps supporting rich features for creating and managing accounts, earning loyalty points, providing reviews, engaging with customer support, other customers and more. While mobile apps for retail are nothing new, many of the first-generation apps are being replaced with apps supporting creative and elaborate digital interaction use cases. These new apps allow merchants and retailers, regardless of sector, to engage with customers in a digital environment, in order to build brand loyalty and engagement and drive towards greater monetisation with enhanced ease-of-use and personalisation.

This shift towards digital economy is fueling the growth of the mobile payments industry and it's becoming a beacon for fraudsters to attack traditional brick and mortar merchants. In fact, **The Mobile Payments and Fraud: 2018 Report** stated that detecting fraudulent orders is one of the top three challenges for merchants in the mobile channel.

Card Present versus Card Not Present = Chargebacks

As brick and mortar merchants make this digital transformation and begin to accept card-not-present and mobile ecommerce, they become exposed to all types of fraud schemes and chargeback programmes that can cause disruption and large financial and brand loyalty losses.

When brick and mortar merchants experience fraud in their traditional card-present environment, the liability of loss is generally on the card issuer if the merchant supports EMV transactions. In a card-not-present (CNP) environment, however (online, mobile web, or mobile app), the liability for a fraudulent transaction now falls to the merchant. This places the merchant at risk of new fraud tactics, potential chargebacks, and greater financial losses.

With a new focus on creating digital accounts for their customers, traditional brick and mortar merchants are also exposed to all types of new fraud, including:

- **Account takeover:** Gaining access to an established digital account using compromised credentials (username and password) allows a fraudster to take advantage of the value of that account. This may include using the saved payment method or loyalty points to make purchases.
- **Loyalty reward points fraud:** Because reward points can work like cash, fraudsters identify weaknesses in the system and steal reward points to sell them.
- **eGift cards fraud:** Considered low-hanging fruit, electronic gift cards are easily converted into cash, a key requirement for fraudsters. They sell them at a discount, with the merchant responsible for the resulting chargebacks and any merchandise or services provided for the value of the gift card.
- **Promotion fraud:** Launching a promotion can often capture the attention of fraudsters who are skilled at identifying ways to get around policies or offer limits. →

Approach to fraud protection

Brick and mortar businesses navigating towards a digital transformation need to deploy a fraud strategy that is multi-layered and specifically accounts for card-not-present fraud.

An underpinning technology for stopping CNP fraud is machine learning. Machine learning combines data, context, and feature engineering to allow organisations to evaluate the risk of a particular digital interaction or purchase. Machine Learning, a form of artificial intelligence, allows fraud prevention solutions to "learn" on their own and continually improve results. In order to stop a card-not-present payment, there are two critical types of machine learning that, when combined, provide the best fraud prevention foundation.

- **Unsupervised Machine Learning.** Unsupervised learning does not require outcomes, so it can learn without waiting for the completion of a three-month chargeback reporting cycle. This type of learning often relies on clustering, peer group analysis, breakpoint analysis, or a combination of these. This enables fraud prevention solutions to detect patterns and anomalies rapidly within extremely large sets of data.
- **Supervised Machine Learning.** Supervised learning uses outcome-labelled training data sets to learn. Models include neural networks, Bayesian classifiers, regression, decision trees, or an ensemble combination. Massive amounts of data run through defined models to assess risk outcomes.

Brick and mortar merchants that deploy a mobile app need to account for a new world of risk through digital fraud attacks. There are great benefits to investing in digital engagement channels, however, with those opportunities comes risk. By addressing fraud with a holistic strategy, merchants can authenticate a user, identify fraudulent behaviour, and stop fraud before it influences the bottom line and diminishes the merchant's brand. By building a level of fraud prevention in their mobile apps, brick and mortar merchants are empowering decision makers with data to make informed decisions and to mitigate fraud before it impacts the businesses' bottom line.

About Kount: Kount's award-winning fraud management, identity verification and online authentication technology empowers digital businesses, online merchants and payment service providers around the world. With Kount, businesses approve more orders, uncover new revenue streams, and dramatically improve their bottom line all while minimizing fraud management cost and losses and protecting consumers. Through Kount's global network and proprietary technologies in AI and machine learning, combined with policy and rules management, companies frustrate online criminals and bad actors driving them away from their site, their marketplace and off their network.

www.kount.com

Click here for the company profile

Covery

Next Generation Fraud Prevention Platforms Leverage ML to Secure Payments

About Pavel Gnatenko: Pavel has a master's degree in intellectual systems for decision-making. He is a risk management expert with more than seven years of experience in the fintech industry. Currently, Pavel is focused on developing Covery - next generation of risk management platforms.

Pavel Gnatenko | *Risk Management Expert* | Covery

As fraudsters follow the growth of the cashless economy online, anti-fraud companies are building powerful tools and techniques that mine various data for fraudulent behaviour patterns.

Fraudulent attacks are getting to be more sophisticated and inventive. Once a new solution against fraud is developed, fraudsters immediately find a new loophole. And it seems that the risk professionals are always a step behind.

Machine learning can be used to help solve this problem, but at the moment it is impossible to completely abandon human intervention.

Rule-based and machine learning approaches complement each other because machines can analyse a larger volume of characteristics, based on the context, while risk analysts can create models that are easily understood by humans, unlike the machine-learning approach alone. Each industry has its own unique set of features and each fraud prevention system aims to adapt them to avoid false positives (good customers identified as fraudsters) and false negatives (fraudsters identified as good customers). Moreover, the risk system needs to periodically be examined by risk managers and afterwards tuned, for example, if online merchants sell new products or make frequent changes to their billing logic.

The power of supervised and unsupervised machine learning

A machine learning solution needs access to a big store of historical data to train its models and increase the probability that it will uncover patterns of new suspicious activity. The more data, the better the system becomes at detecting and preventing fraud.

The machine learning process contributes to the learning of non-linear combinations of latent characteristics and their combinations that lead to predictiveness enhancement.

There are two approaches that are used in machine learning: ***supervised*** and ***unsupervised learning***. The first approach is the most common and widespread.

With the supervised approach, in the beginning, a risk analyst creates a machine learning model based on historical data. Then, with new transaction data, the algorithm creates potentially right baskets: fraud and not fraud. After that, the system collects external signals such as fraud alerts, chargebacks, complaints etc. Based on that information, the algorithm starts looking for new unrecorded dependencies. Finally, the model starts retraining. Consequently, all the risk analysts are one step behind the game, thus, the cycle continues and with time new techniques emerge.

Unsupervised learning is regarded as an alternative to supervised learning. These algorithms infer patterns from a dataset without reference to known or labelled outcomes. Unsupervised learning allows risk analysts to approach problems with no exact idea about what the result will look like. One can derive structure from data where they don't necessarily know the effect of the variables. With unsupervised learning, there is no feedback based on the prediction results. But it can divide data on the basis of anomalous behaviour and then risk analysts can apply well-known supervised approaches to this data. ➔

Therefore, unsupervised machine learning is more applicable to real-world problems and can help to solve them when risk managers are constantly one step behind the fraudsters.

Why use machine learning in payment fraud prevention?

When it comes to detecting and fighting online payment fraud, several advantages become evident:

- it facilitates real-time decision-making and improves the experience for customers;
- it improves accuracy of classification;
- it helps detect new fraudulent behaviour;
- it provides a more rapid response to real-world changes.

What can the best fraud prevention solutions do

The most advanced fraud prevention services use both rule-based and machine learning approaches, including unsupervised techniques, with an industry focus and an adaptation for the business' individual characteristics and customer needs. The result is a solution that makes more accurate decisions for each industry and every customer. One of the companies working in this space is called **Covery**. Risk analysts can customise any combination of data patterns we call 'features' that can be applied to a specific business needs. Covery can also accept any non-payment data in any user action to supplement the profile with missing details to analyse by using both rule-based and machine learning models for more precise decisions.

So what is Covery?

Covery is a global risk management platform helping online companies solve fraud and minimise risk. The company focuses on the versatility of the product and its adaptability to each type of business, based on the individual characteristics and customer needs using both rule-based and machine learning approaches. Covery works with high-risk as well as with low-risk industries to find the right solution for every customer.

What Covery offers to help with fraud prevention:

- wider coverage of user actions for analysis;
- flexible customisation of data patterns;
- usage of any additional data for analysis;
- rule-based and machine learning approaches;
- functionality to work with loyal users to increase revenue;
- custom machine learning models creation;
- custom functionality upon request;

About Covery: Covery is a global risk management platform helping online companies solve fraud and minimise risk. We focus on the universality of our product and its adaptation to any type of business, based on the individual characteristics and customer needs using both rule-based and machine learning approaches.

www.covery.ai

Click here for the company profile

Conclusions

Fraudsters are always developing new tricks and risk managers don't always have the time to adapt to new changes. Machine learning has long been expected to help solve the problem of preventing fraud, but the majority of solutions are still on the path of development. So Covery's main goal is to solve the problem when risk managers are constantly one step behind the fraudster.

Money EUROPE 20/20

Europes's biggest FinTech event is back in Amsterdam.
3 - 5 June 2019, The Rai

europe.money2020.com

Best Practices in the Fraud Management Space

Ethoca

Collaboration Paving the Way for Ecommerce Customer Experience

About Keith Briscoe: Keith Briscoe leads Ethoca's global product and marketing functions, a role spanning the development of Ethoca's suite of collaboration-based fraud/chargeback mitigation and transaction acceptance solutions, as well as integrated marketing programmes. His mandate includes product strategy and management, new product innovation, competitive analysis, experiential marketing, integrated marketing campaigns, public relations, analyst relations, content strategy, and stakeholder communications.

Keith Briscoe | *Chief Marketing Officer* | Ethoca

Goodbye fraud, hello customer experience

If the headline to my editorial caught you by surprise, let me explain. While we're not kissing ecommerce fraud completely goodbye anytime soon (courtesy of those increasingly organised fraudsters, confused customers, and savvy consumers looking for ways to game the system), the payments industry is continuing to direct its focus toward the far more lucrative domain of 'customer experience'.

If 2018 has shown the payments community one thing, it's that we're at a critical inflection point and moment of decision as an ecosystem. As I've talked to payments professionals this year and closely followed the lightning-fast pace of change, the nature of this key 'moment' is coming into sharp focus.

The pendulum shift from fraud to customer experience

The CNP fraud conversation continues to shift increasingly to defining moments of customer experience. While fraud is no longer the central concern, it's still very much part of the picture as the industry continues to cope with a rampant 'friendly fraud' (or false claims) problem. Ethoca's assessment is that the CNP chargeback problem is estimated at USD 50 billion, comprised of a combination of blended OPEX for both merchant and card issuer, and lost value on transactions that are falsely disputed by cardholders (sometimes unwittingly, but increasingly abusive in nature). As a blended average across all merchant categories, friendly fraud is hovering in the 30 to 40% range, but it's most acutely felt in digital goods where it can exceed 90%.

The most staggering fact is that while USD 50 billion is a headline-grabbing number, it pales next to the lost transaction value and customer insult factor that comes with false declines – when good transactions are falsely rejected due to apparent fraud risk. Aite Group estimates that false declines are costing the industry USD 331 billion annually, and that number is set to rise as the pervasive influence of friendly fraud continues to wreak havoc with effective fraud decisioning.

The compounding regulatory ripple effect

One of the biggest ironies of 2018 is that the rise in customer experience together with cardholder protection are reaching a crescendo just as the regulatory environment is about to kick into motion a series of changes that will potentially make it harder than ever to create a frictionless customer experience. Enter PSD2 – particularly the Strong Customer Authentication (SCA) component of the updated payment directive release by the EBA.

When two-factor authentication becomes mandatory on all transactions over EUR 30, the industry will be waiting with bated breath to measure the impact of customer conversion and declines. It's important to remember that potentially 30% of all customer declines are never tried again on another card in the cardholder's wallet. And while SCA exception scenarios exist when fraud rates can be held in check at a PSP or acquirer level, it will prove to be very challenging for ecommerce merchants to realise that benefit with so many false claims in the system. →

3DS 2.0 holds the promise of delivering higher acceptance rates as long as merchants can get comfortable with sharing extended data fields with card issuers to benefit from liability shift. However, in parallel with this key question, there is a lot of chatter about the 'death of fraud detection' given that merchants can simply accept every transaction and let 3DS liability sort out the rest. That would be a tremendously short-sighted move, ultimately straining the delicate card issuer – merchant acceptance balance.

For a start, this approach would trigger more step-up authentication at the card issuer, introducing increased friction – and abandonment – into the purchase process. In addition, facing increased losses as a result of liability shift, card issuers' acceptance and fraud detection models would likely decline more. Once again, we're seeing all of this potentially set the stage for anything but a good customer experience. Creating customer habituation will be key (ease of use, minimal friction and virtual invisibility). But it must be balanced with responsible and equitable behaviours from both merchants and card issuers and enabled by innovative technology that encourages productive, value-based collaboration.

The case for collaboration

So where is all this heading? During no other period in the history of payments has the time been more right for industry collaboration to solve the most pressing problems in ecommerce. The rise of what we at Ethoca call 'bi-lateral rich data exchange' is optimally positioned to solve these increasing challenges. Here are three recommendations for solving the most pressing customer experience and transaction acceptance challenges heading into 2019:

1. **Take the noise out of the system** – The tricky thing with friendly fraud is that it's virtually impossible to detect with typical fraud detection tools because it's largely behavioural in nature. It simply doesn't 'look' like fraud, because it isn't. Making merchants' deep purchase and account insight available to card issuers' mobile applications and to call centre agents – at the pivotal moment of customer concern – is a critical first step in helping customers understand what they bought. The result: better fraud decisioning (less garbage in means higher-performing detection systems), fewer false declines, fewer fraud claims, and improved customer experience.
2. **Set the stage for 'post transaction customer experience'** – Utilising rich data and intelligence sharing between card issuers and merchants to solve for dispute challenges is just step one. Think about where this goes from here: when cardholders have access to their consolidated digital receipts in the bank's mobile app, that's where customer experience enters 'next level' territory. That digital journey should matter as much to banks as it does to merchants, laying the foundation for highly relevant cross-sell opportunities and deeper engagement over the course of the purchase journey.
3. **Build the business case incrementally** – One of the biggest challenges in realising the full potential of bi-lateral rich data exchange between card issuers and merchants is finding the 'wedge' use case(s) that prove the value through an incremental approach. Ethoca's view is that by starting with the biggest pain points – moments of dispute or concern that can be instantly resolved with real-time intelligence 'in the moment' – card issuers and merchants alike will become increasingly comfortable with sharing intelligence that drives the best possible customer experience.

At Ethoca, we're welcoming 2019 with open arms and excitement: the times, it seems, have caught up with collaboration.

RISK IDENT

Felix Eckhardt, Managing Director (CTO), and Piet Mahler, COO, RISK IDENT consider some of the key payment, fraud prevention, operational, and regulatory issues for European merchants with aspirations of doing business in the US.

About Felix Eckhardt: Felix Eckhardt was with RISK IDENT at its inception. Initially taking up the position of senior software engineer, he helped RISK IDENT get on its feet as the chief architect behind the company's second fraud prevention product, FRIDA. A year after the company's founding, Felix became the CTO and remained in the position until he moved to Australia in 2016. While abroad, he acted as Senior Software Developer, developing data-driven solutions for telecoms and marketing industries for two years.

About Piet Mahler: Piet Mahler is the COO at RISK IDENT, leading the strategic direction of the company alongside the CTO, Felix Eckhardt. He is responsible for the development of the business side of the company, having previously held the position of VP Operations & Business Development, helping lead the company's international growth.

Felix Eckhardt | *CTO* | RISK IDENT

Piet Mahler | *COO* | RISK IDENT

Let's start with payments. What do European merchants need to be aware of when expanding overseas?

In the US, payments reflect consumer behaviour. There are generally fewer standard payment methods than in Europe, and the majority of payments are made via credit card rather than direct debit or money transfer.

These payment types may present some difficulties from a fraud perspective – for example, making it more difficult to claw back disputed funds.

One economic factor is the interchange fee on credit cards. Unlike Europe, the US does not have a cap on these charges, which is why the average interchange fee in the US is 1.73%, compared to 0.96% in Europe. Interchange fees on debit card transactions were capped in 2011 by the Durbin Amendment, but this does not apply to credit cards.

How does Europe compare to the US from a fraud prevention perspective? How do the strategies for combatting fraud differ?

In some respects, Europe and the US are similar when it comes to payment fraud. The majority of merchants on both sides of the Atlantic review fewer than 10% of transactions and the reject rate is around 3%.

The overall fraud rate in the US is higher though. One reason for this is that in Europe fraud patterns are more recognisable, since they tend to come from specific countries and merchants. In the US, fraudsters have more opportunity to blend in and find sophisticated ways to get around prevention mechanisms.

It is also easier for fraudsters to build profiles for fraud due to the availability of data in the US, where the focus tends to be on payment validation rather than identity verification. →

> *"The majority of merchants on both sides of the Atlantic review fewer than 10% of transactions and the reject rate is around 3%.*

European merchants tend to rely on vendors for fraud decisions, whereas in the US merchants rely on the vendors for the platform and the merchants figure it out themselves. This seems to be especially true for larger merchants.

Our research has found that the variety of fraud reporting structures in the US is quite pronounced. These reports address different corporate priorities and have a general lack of consensus. This is usually how vulnerabilities that can then be exploited open up.

What operational considerations should merchants focus on when expanding overseas?

US consumers are demanding. Many will make purchases during their commute and they expect next day delivery from all merchants, even those based outside the US. Many of them will not consider where the merchant is based when making a purchase online. Having a US fulfilment house is a consideration.

In Europe, it is critical to offer local payment options to keep conversion rates high. Consumers expect to be able to pay with all major payment types with national differences. Missing payment types lead to abandonment.

GDPR came into effect this year. How does the US differ from Europe when it comes to regulation?

There has been a great deal of talk about the General Data Protection Regulation (GDPR), but European data privacy rules and attitudes have long been far stricter and more discerning than in North America.

The other big change in online commerce in Europe is the Second Payment Services Directive (PSD2). Combined with the GDPR, it provides greater choice for consumers in how they can pay and control their finances, while also aiming to modernise approaches to security and privacy.

One difference is a call for a minimum of two-factor authentication, whereby a consumer would not just be asked for a password, but may be asked for either a biometric scan or for authentication via another device, such as a smartphone. Another example is that US merchants have collected data just because they could, but this is an unnecessary risk and in many cases businesses don't know what to do with this data. Now they have to inform customers clearly about the need and how they manage data protection.

About RISK IDENT: RISK IDENT is an anti-fraud software development company based in the US and Europe that protects companies within the ecommerce, telecommunication, and financial sectors. RISK IDENT's machine-learning software uses sophisticated data analytics to block any kind of fraud, all with human-friendly user interface that simplify a fraud prevention team's decision-making process.

www.riskident.com

Click here for the company profile

Data protection is also a consideration in the US, where individual states often have their own rules, in addition to national standards. For example, the FCC is in charge of the rules concerning what data internet service providers can and can't sell; health data is protected under the federal Health Insurance Portability and Accountability Act, and the Federal Trade Commission enforces the Children's Online Privacy Protection Act.

Ecommerce in the US is worth almost half a trillion dollars annually, according to the US Commerce Department. In Europe, it is worth over half a trillion euros and growing fast.

Cross-border commerce is the Holy Grail for retailers; tune your fraud prevention today to ensure it doesn't become the same for the fraudsters.

Emailage

Are You Ready for the New Era of Online Payments?

About Amador Testa: Amador is Chief Product Officer at Emailage. He is an industry expert in online fraud, identity theft and cybercrime. Before Emailage, he was the head of fraud for card acquisitions at American Express and later led global fraud prevention divisions at Citigroup. Amador enjoys playing tennis, running marathons and traveling with his family.

Amador Testa | *Chief Product Officer* | Emailage

Traditionally, when we talk about the approval of online transactions, merchants are the ones who have the majority of 'rich' data.

By that, I'm referring to merchants having access to elements such as customer demographic info, name, email address, and IP address of the customer submitting the transaction. Also included is the shipping address, along with what type of products are being purchased.

The hitch in this process is that when merchants request authorisation from the issuing bank, those issuing banks don't have access to the same data. The data they can see has historically been very limited. The basic things that issuing banks can see are:

- What is the line of credit for that card?
- Is that transaction over the limit?
- Has that card been used before in that industry?
- Has that card been used at that merchant before?

The transaction amount, and in certain cases the name and billing address associated with the payment method, which can help in the authorisation process, may also be present.

Here's the problem

The lack of visibility for issuing banks into this important customer information can generate significant impacts on the authorisation process. These effects are especially magnified in the Central and South American markets, where a very large percentage of online transactions are declined, even reaching 20% or more in certain industries.

In the US, the numbers are much lower, but the impact is still there, nonetheless. There is an exception, though, when the Issuing Bank is also the Acquirer, meaning they have a relationship with the card holder as well as the merchant.

These types of relationships allow more data to flow than a simple credit card and name/address information, such as the email and IP addresses, and other details about the order, which have proven to be indispensable in allowing more precise decisions that benefit all parties involved.

For customers, orders are approved more quickly with less disruption. For merchants, this translates into more revenue, as a larger portion of orders is approved. →

Big changes to come

There are key changes on the horizon for issuing banks, allowing them to validate digital identity of their customers.

Version 2.x of the 3-D Secure protocol is the first to require merchants to send the email address of customers to the issuer. While there are many other data fields also included, the email address is important because it is almost invariably used to confirm the purchase. This means that if fraudsters use the address associated with the card, the cardholder will be informed that an order has been placed. Criminals can avoid this by using accounts under their control to place orders. Email can, therefore, be a vital indicator of fraud. But it's not as simple as checking that the email address matches that held by the issuer. Globally, it is estimated that there are 1.75 accounts per email user and this figure is higher in the developed world with users typically having three active accounts including a work email address. Spotting a new or unrelated email address can really help.

It's also important to know whether a specific address has been involved in a previous fraud. While email address checking is no silver bullet for ecommerce fraud, it can be a powerful tool when combined with other data and analytics during the authentication or authorisation process.

emailage®
The Global Hub of Email Intelligence

About Emailage: Emailage, founded in 2012 and with offices across the globe, is a leader in helping companies significantly reduce online fraud. Through key partnerships, proprietary data, and machine-learning technology, Emailage builds a multi-dimensional profile associated with a customer's email address and renders a predictive risk score. Customers realize significant savings from identifying and stopping fraudulent transactions.

To learn more, visit: **www.emailage.com**, @Emailage on Twitter, or the company's **LinkedIn page**.

Click here for the company profile

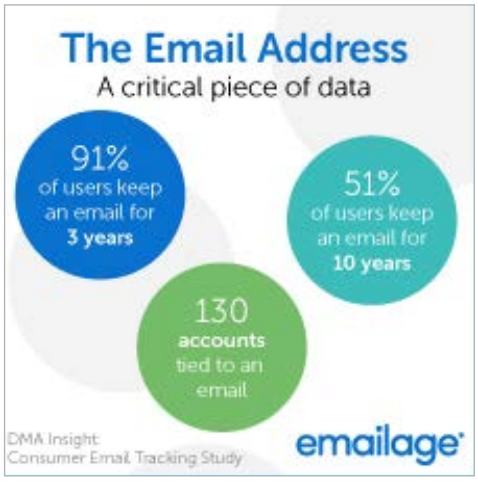
Risk scoring of email addresses

While using email as a factor in risk assessing payments is new to issuers, Emailage has a history of helping merchants counter the threat of fraud in ecommerce. Since 2012, Emailage has offered fraud risk assessment built around the email address.

We utilise a predictive risk score based on machine learning algorithms combined with a cross-industry and cross-sector consortium database. This approach offers merchants the ability to mitigate fraud with negative signals while using positive signals to approve good customers. The roll-out of 3-D Secure 2 and the implications of Strong Customer Authentication in the European Union will mean that both the obligation and the capability to fight fraud move to card issuers.

Conclusion

Card issuers are faced with a challenge – how will they balance customer friction and fraud prevention? The businesses which have better fraud risk analytics and better data on which to make decisions will do better. Merchants have already discovered that email address is an effective fraud risk factor in ecommerce; it is now time for the financial services industry to learn lessons from them.



Emerging Payments Association

Account Takeover via Hacking Bots (The Rise of the Bots)

About Neira Jones: Neira advises organisations on payments, fintech, regtech, information security, regulations and digital innovation. She holds a number of Non-Executive Directorships and Advisory Board positions and is on the Thomson Reuters UK's top 30 social influencers in risk, compliance and regtech 2017 and the Planet Compliance Top 50 RegTech Influencers 2017.

Neira Jones | *Ambassador* | Emerging Payments Association

An increasingly mobile & digital landscape

As mobile transactions now account for **58% of total transactions**, mobile is now fuelling each stage of the customer journey and has become the preferred method of interaction. Across industries, almost two-thirds of all account creations now come from a mobile, whilst in financial services, mobile transactions make up 61% of all account creations and 66% of all account logins.

With the global push for digitisation, online transaction volumes are relentlessly increasing, mimicked by a corresponding surge in cybercrime and automated attacks. Compounded with the regulatory push for disclosure, individuals have resigned themselves to the dramatic headlines and alarming statistics.

Technology as an enabler: opportunity knocks...

The more consumer behaviours change and adoption of new technologies increases - such as machine learning (e.g. AI driven financial apps, chatbots), the IoT (e.g. payment wearables, home assistants) - the more criminals find additional opportunities to exploit vulnerabilities. Indeed, the 21st century has given fraudsters an ideal playground with the combination of digital interactions, the systemic failure of organisations to keep pace with the security measures needed for new technologies, readily available personal data that can be harvested from the many data breaches that have or have not made the news, and the willingness of many merchants to relax their risk controls during peak transaction times to approve more orders (such as during world sporting events or holiday periods). Moreover, as criminals also have the opportunity to capitalise on new technologies and automated tools, this melting pot of opportunity has enabled them to find new ways to hide behind large transaction volumes, leading to spikes in bot activity (ThreatMetrix Q2 2018 Cybercrime Report).

A complex regulatory landscape

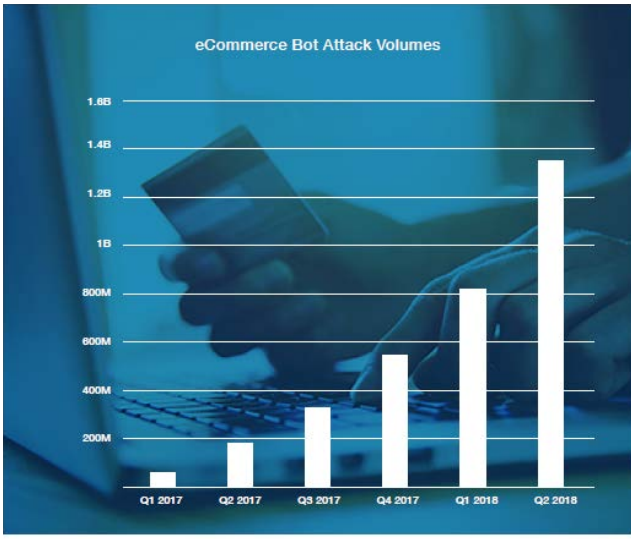
As payment industry reforms (e.g. 3DS 2.0 and Open Banking worldwide, or PSD2 in Europe) try to promote innovation and reduce friction whilst providing secure payment interactions, data protection regulations (such as the GDPR in Europe or the CCPA in California) apply even more pressure on businesses that handle personal data.

To meet the regulatory challenge and manage risk effectively, organisations must get as close as possible to a single end-to-end view of the customer, regardless of service/product, channel or device. And they must do this as seamlessly as possible. In other words, businesses must be able to distinguish between genuine customers (who are increasingly ubiquitous) and fraudsters (who are increasingly able to mimic genuine customers).

The automation era

Indeed, stolen data (and identities) will be used by criminals for two main purposes: *opening new accounts* (which can lay dormant for periods of time and then used to make payments using stolen card details) and *taking over existing accounts* (to purchase goods and services, steal credentials and payment details). Large *ecommerce* retailers are a target of choice for automated bot traffic, which makes use of readily available stolen identities and capitalise on the fact that individuals will often reuse passwords across many sites (aka "Credentials Stuffing"). ➔

Automated bots enable criminals to launch attacks that keep trying credentials until they match an existing account, with very little effort.



Source: ThreatMetrix Q2 2018 Cybercrime Report

By contrast, the *financial services* industry has always been heavily regulated, and security and fraud prevention mechanisms are generally stronger than in other industries. It is no surprise therefore that the preferred attack method is through social engineering (e.g. tricking customers into transferring funds to a mule account, or giving away credentials). A notable exception to this is that *fraudsters* see fintech providers as easier targets than traditional financial services companies due to the fact that fraudsters attempt to exploit new and emerging platforms to exploit gaps in process and infrastructure (e.g. "Loan Stacking" - where new loans are applied for using an infiltrated account, using one loan to pay off the next until the loan value is inflated to the maximum amount available, which is when the criminal defaults on payment), targeting account logins and payments transactions.

Challenges and opportunities

As consumers continue to adopt new and emerging technologies, the challenge is to balance customer experience with security. This will mean that businesses will have to ensure that they deploy dynamic approaches to counter the proliferation of stolen identity credentials and advanced device and identity spoofing techniques which allow fraudsters to bypass the most complex online application procedures. Indeed, recognising legitimate customers across industries and channels will also fuel growth and opportunities. This also means that businesses must use a variety of fraud detection and prevention methods, stop relying on passwords as their top form of authentication and look beyond retrospective transaction analysis towards real-time and predictive consumer behaviour analysis, as well as moving beyond rules to context and attributes. Moreover, the lack of digital identity integration with wider customer engagement strategies will lead to fragmented customer experiences and customer attrition, the inability to capitalise on customer data to inform decision-making and enhance the overall customer experience, as well as to data privacy challenges. Real-time solutions combining multiple data points (e.g. device information, biometrics, contextual, predictive, and behavioural information etc.) will help businesses better recognise their customers - rather than challenge them - and will also help identify anomalies such as account takeover and automated bot traffic.

Merchant Risk Council

Paul Kuykendall depicts his vision of MRC's future growth opportunities and the way this community evolved in order to support merchants in fighting payments and commerce fraud.

About Paul Kuykendall: With over 20 years of experience in global payments and fraud technology, Paul came to the MRC as the VP of Payment Platforms for the world's largest ticketing company. He is a subject matter expert on payment processing, data security, compliance, and risk mitigation. Paul's prior MRC involvement includes various committees, regional boards, and the Global Board of Directors.

Paul Kuykendall | *CEO* | Merchant Risk Council

Could you please provide our readers with some insights into your professional background, prior to joining MRC?

My degree is in mechanical engineering, so I love to solve problems. However, I started my payments career as a software engineer at Ticketmaster, which has grown into the largest and most comprehensive ticketing platform in the world. We built our payments and ecommerce platforms from the ground up, for ultra-high performance and scalability. About midway through my journey at Ticketmaster, I caught the fraud-fighting bug, and dedicated much of my time to making our payments and risk teams work closely together to disrupt the fraudsters. We developed internal systems and partnered with other great companies to fight back.

As an ecommerce leader, with extremely high stakes in fighting fraud, my organisation joined the MRC as a Merchant Member where I soon became very involved in the MRC community, engaging as a conference speaker, a committee member, and ultimately serving on its Board of Directors.

Merchant Risk Council is now a well-known association among fraud and payments professionals, firmly rooted in the industry. How did everything start and what problems were the founding members looking to solve back then?

This whole thing started almost two decades ago. In fact, the MRC celebrates its 20th anniversary in 2020, and to this day continues its vision of making commerce safe and profitable everywhere. It all began when a handful of online retailers got together to discuss their challenges in fighting fraud.

The Internet was brand new, with huge potential for sales, and in turn, created a new channel for criminals to infiltrate and take advantage. This merchant group met in person a few times a year, and later formed the organisation known now as the Merchant Risk Council. As ecommerce exploded, so did fraud, and the demand for online solutions and technology to fight it. The MRC naturally grew in membership and expanded its reach to include solution providers, issuers, card brands, law enforcement, and other industry partners. Today the MRC consists of a diverse mix of nearly 550 member companies representing a wide variety of industries, technologies, and services. What's really cool is that nearly all the founders are still very involved with the MRC, either as merchants or solution provider member organisations. Collaboration started everything and continues to be what it's all about! →

> *"Our mission is engagement within our community. MRC leads the industry with information about fighting fraud, reducing risk, and optimising payments.*

What were the key themes on the agenda of US fraud and payment managers for this year?

Improving the customer experience is an interesting theme that is emerging from the merchant community and is reflected in upcoming conference agendas and the ongoing conversation. The conflict between checkout friction and sales conversion is always a point of discussion. Identifying fraudulent behaviour without rejecting or offending good customers is critical because the market is so competitive. Identity verification, machine learning, deep analytics, and chargeback management are all gaining prominence in the conversation. But, as always, the focus is on people getting better at what they do, learning from their peers, and evolving together with the industry.

How does MRC help new entrants in the industry cope with the rapid changes in the payments fraud and risk environment?

Our primary mission is engagement within our community. MRC leads the industry with information about fighting fraud, reducing risk, and optimising payments. We offer and are expanding our online education courses called RAPID Edu, which is short for Risk and Payments Industry Development Education. This is a great leg-up for professionals new to the payments and fraud industry because they can take educational courses at their own pace, and on their own schedule, at a time convenient to them day or night. Currently, the MRC offers a Chargeback Essentials course and will soon be releasing a Fraud Essentials course followed by a Payments Essentials course in the coming year. We also encourage collaboration through our mentor programme, where new folks can meet experienced professionals and get a quick introduction to key people and concepts that will improve their skills. Our website is packed with case studies, webinars, surveys and whitepapers (as well as other relevant content to help educate) and our community forums spur important conversations. Last but certainly not least, we offer four annual, best-in-class conferences in the US and Europe as well as regional networking events throughout the year. We truly have so many avenues through which our merchants can learn and grow.

MRC Building Better Commerce
Fraud & Payments Professionals

About Merchant Risk Council: The Merchant Risk Council (MRC) is a global trade association providing a platform for ecommerce fraud and payments professionals to come together and share information. As a not-for-profit entity, the MRC provides year-round support and education to members by offering access to proprietary benchmarking reports, whitepapers, presentations, and webinars. The MRC hosts four annual conferences in the US and Europe, as well as regional networking meetings for professionals to build better business connections, exchange best practices, and share emerging trends. The MRC is headquartered in Seattle, WA and has an office in Dublin, Ireland.

www.merchantriskcouncil.org

How do you see this industry evolving in terms of both challenges and innovations and how does this evolution align with MRC's plans for 2019?

'We are the MRC community and together we evolve' was the theme of our autumn conferences this year, and we totally embrace it. The business of fighting fraud is changing at a rapid pace, and merchants must adapt together. The fintech industry is bursting at the seams with new and better ways to identify and stop fraud. The very cool thing about the collaboration that the MRC generates is that we, as a community, solve problems, and share the solutions. It's an arms race, for sure. We know that fraudsters collaborate. They share tools and resources on the dark web. They exchange information about what works for them, and what doesn't. The best way to beat them is for merchants, large and small, to work as a team. That's what the MRC is all about.

MRC Building Better Commerce
Fraud & Payments Professionals

Merchant Risk Council

Leading Global TRADE association for eCommerce fraud and payments professionals.

The MRC provides year-round support and education to members by offering access to proprietary benchmarking reports, whitepapers, presentations and webinars. The MRC hosts four annual conferences in the US and Europe, as well as regional networking meetings for professionals to build better business connections, exchange best practices and share emerging trends.

MRC MEMBERS EXPERIENCE

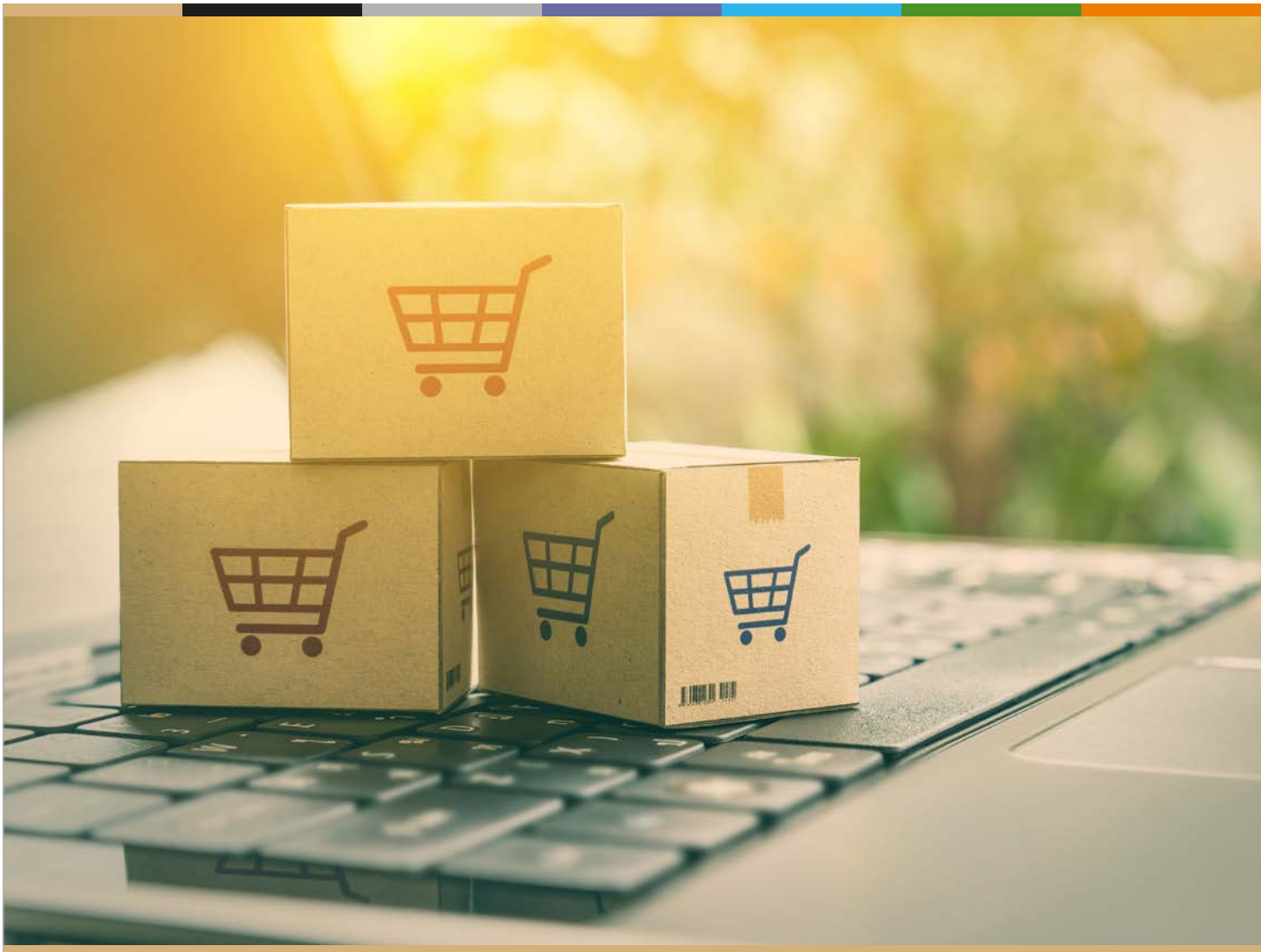
29% LESS FRAUD AND HIGHER CONVERSION RATES THAN NON-MEMBERS.

ASK US HOW!

MRC Building Better Commerce
Fraud & Payments Professionals

#ProudlyACommunity

merchantriskcouncil.org



Best Practices of Mitigating Fraud in Ecommerce – the State of Affairs in Ecommerce Verticals

Fraud in Ecommerce – Diagnosis and Treatment

Mirela Ciobanu | *Senior Editor* | The Paypers

Ecommerce as a whole continues to be a prime target for **monetising stolen identity credentials** harvested from **data breaches**. Stolen data (and identities) will be used by criminals for two main purposes: **opening new accounts** (which can lay dormant for periods of time and then used to make payments using stolen card details) and **taking over existing accounts** (to purchase goods and services, steal credentials and payment details).

Once fraudsters have stolen account credentials, they don't wait around, but **use them to commit account takeover (ATO)**, **Sift Science security specialists** warn us. For businesses that experience the highest rates of ATO, a compromised user's account activity increases an average of 22x within a week of the takeover. Fraudsters use stolen credentials as much and as quickly as they can before the user or business redeems control of the account.

As mobile is becoming the key enabler at almost every stage in the customer journey, fraudsters have now realised that if they perform a **SIM swap**, or even **port out a telecoms account service**, they can **gain the ability to not only add services to the telephone account**, but also **use the phone number to intercept and approve financial transactions**, compromising both the victim's financial services and their telephone account, says Jason Lane-Sellers, CFCA President & Director.

SIM swap fraud is largely made possible due to the fact that customers are able to switch SIMs while carrying their current phone number with them. Fraudsters exploit this possibility, calling network operators and posing as the victim claiming to have lost their SIM card or needing switch to a new provider. If the fraudster successfully passes the security questions asked by the operator, they will be able to transfer the victim's phone number over to a SIM card in their control.

Another type of fraud encountered in the online luxury industry is **Mail Order/Telephone Order fraud** (MOTO). MOTO is a form of 'card-not-present' transaction, where services are paid for and then delivered via the internet, telephone, or mail. For a Switzerland-based luxury goods holding company, Richemont, this type of purchasing represents 50% of the transactions, and therefore the risk associated with it is increased, as the MOTO channel is also preferred by fraudsters.

Challenges and recommendations

Some key challenges for ecommerce merchants are: balancing an optimised customer experience with low friction authentication, **shortening processing times for orders, the ability to effectively identify good returning customers**, while also maintaining effective fraud control. **Also, with the advent of PSD2 in Europe, businesses need to integrate risk-based authentication with low-friction SCA in order to avoid introducing unnecessary friction into the payment flow**.

One way to do this is through device binding, a process that allows users to transact on trusted devices without repetitive authentications. This occurs through reliable and consistent verification of the transacting device, by registering the device and binding it with a user credential. →

Fraud in Ecommerce – Diagnosis and Treatment

Another way to understand potentially high-risk scenarios in ecommerce/chargeback situations is to create a unique digital identifier for every transacting user, and visualise the relationships between all the entities linked to that user, such as device information, tokenized email address, and other account markers.

Enterprises need to ensure they have dynamic, behavioural analytics-based fraud detection systems in place, which can both identify good returning customers in unusual situations (such as travelling abroad to the World Cup/ Winter Olympics), as well as spotting fraudulent use of credentials, which criminals try to mask by hiding in unusually high transaction volumes. Fraud and risk managers should also take into account quantifying the revenue impact of false positives and poor customer experience due to legacy techniques and policies aimed at reducing fraudulent events. They are advised **by Gartner to consider** an expanded ROI calculation to increase revenue opportunities, as well as reduce potential fraud losses.

Sift Science

The Paypers sat down with Kevin Lee, Trust & Safety Architect at Sift Science, to find out the latest trends and developments in fighting loyalty fraud in travelling industry.

About Kevin Lee: Kevin Lee is driven by building high performing teams and systems to combat malicious behavior. He has worked for the last 10+ years around developing strategies, tools and teams responsible for billions of users and dollars of revenue. Prior to Sift Science, Kevin worked as a manager at Facebook, Square and Google where he lead various risk, chargeback, spam and trust and safety organizations.

Kevin Lee | *Trust and Safety Architect* | Sift Science

Sift Science is a technology vendor for online travel agencies (OTA) that seek to fight fraud. Can you portray your typical customer?

Our typical customers are companies seeking an innovative technological approach to fighting fraud, while also placing equal importance on maintaining an excellent user experience. Customers who have something of the best results with us tend to operate with low-margin, high-volume, instant-delivery business models. They also often have lean fraud teams and rely heavily on automation.

What are these customers currently doing wrong in stopping fraud and what are the challenges they are facing?

In the online travel space, fraud teams must make accurate real-time decisions for high average order amounts, looking at users that are new to the system or don't make bookings very frequently. This is very challenging, because you don't have as much data on these travelers, and there is high financial risk involved in every decision.

Many fraud prevention vendors only look at transaction data, which results in lower accuracy. Behavioral data is extremely valuable for preventing fraud. Imagine this scenario: a legitimate travelers buys flights to Barcelona, spending time browsing for the best deal, choosing seats, checking out hotel packages, and sending the itinerary to family members. It takes a while. In contrast, a fraudster may complete the entire shopping process in two minutes and then log out.

Legitimate users rarely bother to log out of websites. The timing and logging out are two signals that could point to fraud.

Other vendors also use rules that don't scale, are static, and don't adapt to changing fraud patterns. At Sift, our real-time machine learning based on an ensemble of models and 16,000+ signals is a real differentiator.

> *"Loyalty programmes create financial liability for companies, since so many travellers accumulate large unused balances.*

How do loyalty programs work in this industry and how do fraudsters exploit them?

Forget bitcoin – loyalty points are the original digital currency. Loyalty programs create financial liability for companies, since so many travelers accumulate large unused balances. These balances are attractive targets for fraudsters, since they're easy to drain, and you don't need to input payment info to redeem the points. Loyalty fraud is a growing crime, with **11% of card-not-present fraud attacks** on loyalty and rewards points accounts in 2017 – up from 4% in 2016. ➔

In a typical scheme, a fraudster will use stolen login credentials obtained from a data breach or hack to gain access to a traveler's account. Then, they use the "transfer points" option to liquidate the balance. A fraudster may also use stolen credit card information to purchase multiple airline tickets, accumulating a huge amount of loyalty points and quickly redeeming them before the crime is discovered.

Unfortunately, most loyalty programs have minimal security in place to curtail this abusive activity in order to provide the most friction free customer experience as possible. In fact, many companies choose to whitelist these customers in order to circumvent any security checks, which is especially problematic.

How are companies in the travel industry currently fighting/preventing these problems? Does a solution for preventing loyalty and travel fraud truly exist?

Some solutions that travel companies use to prevent loyalty fraud include:

- Setting limits and rules on how fast customers can earn points and spending requirements to accrue points
- Establishing manual review teams to spot abusive behavior
- Checking customer point transactions histories, looking for how long and at what pace a person accrued points, as well as how fast those points were spent
- Introducing 3-D Secure or other verification methods

However, these solutions not only negatively impact the customer's experience – customers don't want to be made to spend a minimum in order to accrue points or have to remember a password to verify their identity – they also require more labor and cost on the merchant's end. **Sixty percent of online businesses are concerned about spending too much on manually reviewing orders**.

A true solution to preventing fraud is multi-layered. It's not just about eliminating fraud, but more about limiting exposure and enabling your top line to grow. At the foundation is the ability to ingest a high volume of data from all stages of the customer journey. Then, you need sophisticated technology like real-time machine learning to uncover patterns in the data, so you can both automate accurate decisions and empower your review team to take the right action on gray-area cases.

About Sift Science: Sift Science is a machine learning company that fuels business growth by empowering world-leading online businesses to drive risk-free user experiences. Sift dynamically prevents fraud and abuse by combining industry leading technology and expertise, a global data network and long-term customer partnership. Global brands such as Twitter, Airbnb, Yelp!, Shutterstock, Jet.com, Indeed and Wayfair rely on the Sift Science Digital Trust Platform for access to a global network of fraud data, 16,000+ fraud signals, and its unique ability to detect and prevent fraud in real time.

www.siftscience.com

Click here for the company profile

About-Fraud.com

Airlines Need Better Anti-Fraud Data

About Ronald Praetsch: Ronald Praetsch is Co-Founder and Managing Director of about-fraud.com. He also consults regularly with merchants, payment service providers, and fraud solution vendors. Before founding about-fraud.com, Ronald spent close to a decade in various payments and fraud prevention roles at Sift Science, Fareportal, Booking.com, and Pay.ON, in both Europe and North America.

Ronald Praetsch | *Co-Founder and Managing Director* | About-Fraud.com

Data breaches at major airlines have been in the news a lot lately, highlighting the increasing supply of basic payment data in the black market economy. British Airways, Air Canada, and Cathay Pacific all lost millions of clients' credit card numbers, email addresses, passport numbers, and more, which will probably be used in attempts to defraud other airlines and travel industry merchants. What hasn't changed, worryingly, is that many large airlines still rely on basic fraud checks that can easily be bypassed by 21st-century fraudsters and have yet to implement more advanced fraud prevention solutions based on richer data sets not yet compromised by these fraudsters.

Many airlines today rely on legacy infrastructure and anti-fraud solutions based on technology developed in the '80s and '90s, such as address verification services (AVS) and card verification numbers (CVN). A quick look at the data available on the open web and in dark web marketplaces would quickly reveal to any payments executive that these identifiers are compromised and can be bought cheaply and in bulk by fraudsters.

Get better data

What are the airlines missing? Today, there are many more classes of data that can be used to authenticate transactions. This includes biometric data, behavioural data, and device identity data. Now, you can determine if a person is who they say they are by authenticating their voice, their thumbprint, or their eye scan. If you are trying to minimise friction in your checkout process, you can authenticate a customer by how they interact with your webpage and/or their device – a technology that is becoming increasingly popular, especially with banks.

You can also add the use of device identity data in fraud prevention, which is becoming commonplace enough that some providers of traditional personally identifiable information (PII) now supply device ID data in their solution offerings as well.

There are dozens and dozens of fraud solution vendors that enable merchants to seamlessly incorporate these new data types into their payment flow. About-Fraud.com regularly updates **a list of these vendors**, filtered by solution type, so merchants should have no trouble locating them. Unlike older fraud prevention tools like AVS, airlines also need not worry about the geographical limits of these solutions. There are at least a couple of solutions active in every major geographic market and all the new data types and the technology they leverage are truly global in nature.

Fully benefiting from automated risk scoring

Airlines should not be late adopters to advanced fraud prevention technology. Their business model leaves them more exposed to fraud than the typical merchant. Currently, airlines use a number of different sales channels, including their websites, online travel agencies, consolidators, and travel agents, but many still only apply one uniform set of anti-fraud rules across these very different channels. Moreover, airline customers come in every shape and form, from locations all over the world. Some customers still plan their trips months in advance, but the entire travel industry is experiencing growing volumes of last-minute purchases by both business travellers and tourists. This makes it very difficult to create a clear rules set that will block the fraudsters without losing a significant number of legitimate purchases. ➔

Unsurprisingly, a recent CyberSource study found that airlines still need to manually review 18% of orders, despite only 12% of manually reviewed bookings ultimately being cancelled. While this represents a significant improvement – over 27% of transactions were manually reviewed in 2014 –, it is still too high. Bringing down the manual review numbers even further would require not just increased automation but smarter automation, ie artificial intelligence solutions fed with enough meaningful data points that they can make decisions not only faster, but also better than the typical fraud analyst.

Data is the lifeblood of fraud prevention

A handful of major platforms have enabled airlines to bring down their manual review rate and adapt to changing and complex fraud trends with automated risk scoring engines that utilise machine learning models to predict transaction risk. But even the most advanced machine learning algorithms won't solve the problem of 'garbage in, garbage out'. Put simply, to dramatically reduce fraud and false positive rates these systems need large amounts of data that can be used to distinguish customer identity and risky transactions.

To cut down on revenue lost to inefficient fraud prevention mechanism, airlines need to spend more time and resources on testing the efficacy of new data types for preventing fraud across different sales channels. The big banks are doing it. Apple and Microsoft are doing it. It's about time the airline started doing this seriously as well.

ABOUT-FRAUD.com

About About-Fraud.com: About-Fraud.com delivers expert knowledge on technology and trends to a global community of a fraud fighting professionals. Fraud management is super complex, with online businesses struggling to understand and keep pace with evolving trends, technology, best practices and providers. To these businesses About-Fraud.com provides market research and consulting services.

www.about-fraud.com

Communications Fraud Control Association

Telecom Fraud – The Impact of Digitalisation

About Jason Lane-Sellers: Jason is a highly experienced fraud professional who has been working in the telecommunications industry for 20+ years, and he is currently President of the Communications Fraud Control Association. He has a wealth of experience within operators and vendors covering fraud, risk & revenue assurance.

Jason Lane-Sellers | *President & Director* | Communications Fraud Control Association

The telecom world is changing, all while enabling the digitisation of services across different sectors; these changes, however, are increasing the fraud risks and threats within the telecom world itself. Due to digitalisation, telecom services can be both the point of attack to initiate fraud, as well as the victim of fraud.

As the phone has become a common authentication point for many financial or ecommerce services, fraud against telecom consumers and the telecom services is rising rapidly. Further **increases in fraud** impacts are **due to the inherent value of the equipment being supplied by telecom providers**, thus becoming attractive targets for the criminal fraternity, as they are items that can be quickly cycled to revenue.

The rise in consumer-based fraud attacks against telecom services is highlighted within the last Communications Fraud Control Association fraud report, which showed a combined value of over USD 11 billion lost to various types of consumer-related attacks, and even this number is thought to be highly underestimated.

Recent years have seen a re-growth in subscription fraud attacks, in order to gain equipment and services. As well as over 300% growth in account takeover attacks in order to compromise the consumer themselves, particularly in relation to financial services.

Although **subscription fraud has been a perennial problem** for almost all service industries, **recent growth has been focused around the use of "credit mules" or synthetic identities**. "Mules" are when a genuine entity has been approached and knowingly passes on their personal details in order to allow them to be used for an account creation. These mules are often recompensed immediately and do not necessarily realise that the details they provide will be used for a fraud attack and may damage their future credit profile. As such, it is difficult for service providers to identify mules as the details being used to create an account are genuine and not falsified.

A synthetic identity is when an identity and a credit profile are created by combining both genuine and fake data in order to set up accounts across multiple services – services which may be very low value, but with small credit interactions. This can then create an impression of a credit active consumer, so when the synthetic ID is used for a major purchase, the credit file and history are apparent and warning flags may not be raised.

The growth of online and ecommerce channels allows the use of "mules" and synthetic identities in high volumes remotely, thus enabling attackers to manipulate thousands of transactions over a short period of time.

Account takeover has been the fastest growing form of fraud for telecoms over the past few years. Much of this is attributable to the changing nature of service provision. Customers now expect instant access to accounts, simplified services, and recognition of loyalty. As such, often accessing and adding services or equipment to existing accounts is faster and simpler, with fewer checks and verifications than opening new accounts. Fraud operatives have targeted such principles ruthlessly. ➔

In the early stages of account takeover growth, a large focus for fraudsters was on the ability to upgrade equipment or add additional connections and equipment to existing accounts – if you could access the customer account, you could perform these actions to gain equipment for resale. However, the growth of digital services across the different markets means that there are other reasons to compromise a telecom account. Taking phone numbers as a case in point, which are increasingly being used as an authentication tool for ecommerce and online financial services, whereby a message or call is sent to the phone/cell to approve an ecommerce or financial transaction. Fraudsters have now realised that if they perform a **SIM swap**, or even **port out a telecom account service**, they can then **gain the ability to not only add services to the telephone account**, but also **use the phone number to intercept and approve financial transactions**, compromising both the victim's financial services and their telephone account. This proves doubly damaging for the telephone provider, as they are seen as responsible for the attack against the financial transaction, as well as for the phone account.

Now, most of the growth in these types of fraud has been driven via the digitalisation of services and provision of apps, online self-service, and digital interactions. Therefore, from a fraud management point of view, in order to start to manage or prevent many of these types of attack, it is **necessary to understand the nature of the customer and digital services**. As these attacks are manipulated across different marketplaces, it can be difficult for traditional service providers to adapt.

Therefore, **telecom providers need to be able to understand and identify their customers in the new digital world**. As we move into the crossover between service provision, access, and utilisation, where people interact with multiple devices, in multiple locations and across services, it has never been more important to be able to profile an entity as a complete digital persona.

Leading organisations in the telecom world are now integrating digital identity solutions in order to protect their customers, authenticate interactions, and prevent fraud attacks.

COMMUNICATIONS FRAUD CONTROL ASSOCIATION

About Communications Fraud Control Association: CFCA is a not-for-profit global educational association that is working to combat communications fraud. The mission of the CFCA is to be the premier international association for revenue assurance, loss prevention and fraud control through education and information. By promoting a close association among telecommunications fraud security personnel, CFCA serves as a forum and clearinghouse of information pertaining to the fraudulent use of communications services.

www.CFCA.org

The most advanced solutions amongst these allow the crowd-sourcing of data across verticals, for a complete digital picture. These solutions enable the provider to openly promote the use of online services, whilst validating data and ensuring trust in interactions across their digital channels. Operators who are not following this trend or approach are quickly becoming the targets of the advanced criminals to a frightening scale.

Emma Mohan-Satta

Sim Swap Fraud – an Attack in Multiple Stages

About Emma Mohan-Satta: Emma has been working in fraud prevention for the past decade developing knowledge across financial services and ecommerce. After working for American Express, she gained experience with a number of fraud prevention vendors and now looks after fraud risk and strategy for a fintech startup called Capital on Tap.

Emma Mohan-Satta | *Senior Fraud Manager*

With ever more finance and ecommerce apps present on our smart phones, SIM swap fraud is a lucrative choice for fraudsters looking to gain access to victim accounts, credit cards, and personal data. Online account providers, from social media to ecommerce and banks, frequently encourage users to add a mobile phone number as part of their "two-factor authentication" strategy in order to secure their users' account access or before allowing users to carry out financial transactions. The mobile phone number linked to the user account is then used to validate that future attempts to access services are made by the genuine customer. But what if a third party has managed to gain control of this number?

SIM swap fraud is largely made possible due to the fact that customers are able to switch SIMs while carrying their current phone number with them. Fraudsters exploit this possibility, calling network operators and posing as the victim claiming to have lost their SIM card or needing switch to a new provider. If the fraudster successfully passes the security questions asked by the operator, they will be able to transfer the victim's phone number over to a SIM card in their control.

As additional personal information about the victim is required in order to complete this kind of attack, SIM swap fraud is frequently the second stage in a wider fraud attack usually starting with targeted social engineering. Potential victims are identified and targeted with phishing emails or calls seeking to discover personal data including passwords and secret answers.

Victims often struggle to tell the difference between these highly personalised and sophisticated requests for information against legitimate communications from their bank or websites they frequently use. Key information such as full names and dates of birth can also be gained by searching social media or other public websites allowing a potential fraudster to quickly complete a profile of their intended victim or victims. This research stage of the attack will often help the fraudster discover which banks or ecommerce sites are used by the victim, and so the fraudster will know which companies to target once the SIM swap stage of the fraud has been successfully carried out.

Once the fraudster has control of their victim's phone number, relatively unlimited access is available to any of the victim's accounts that use SMS messaging as the second factor for authentication. Security texts will be sent to the number now in the fraudster's control, locking the victim out of their phone and their accounts. When successfully combined with social engineering, SIM swap fraud can lead to the equivalent of a "device takeover" attack as the victim's Apple account, for example, can be set up on a new iPhone in the fraudster's control. This is made possible as long as the fraudster possesses all of the vital security answers which will have been gathered during the social engineering stage of the attack and may allow the fraudster to go as far as adding a new fingerprint ID to the victim's Apple account. At this stage, all of the victim's iPhone apps, and therefore financial data stored within those apps, are in the fraudster's hands. →

While the victim is likely to detect the issue relatively quickly when access is lost to their phone number and device settings, putting it right and regaining control of their identity can prove a time-consuming problem while operators and account providers seek to confirm the true identity of the customer. This additional time allows the fraudster to complete their attack and drain the victim's accounts or gain further personal data for carrying out future attacks such as setting up new fake financial accounts in the victim's identity.

Online account providers, particularly in the financial services industry, can look for risk indicators such as a change in device behaviour to identify a change in identity behind the account access. This may lead to taking additional precautionary and verification steps before sending a second-factor text message to a number under the control of a fraudster. Providers may also wish to consider the use of app-based authentication where the device itself, rather than the phone number, forms part of the authentication. When a significant change in device or device settings is detected, additional steps can be taken before sending the authentication code to prevent a fraudster from intercepting this valuable code.

Users can also limit the potential for their own accounts being caught in such an attack by limiting the amount of information they reveal about themselves online and exercising caution when receiving emails or calls purporting to be from their bank. By avoiding the social engineering stage of the attack, the potential for a fraudster to carry out a SIM swap is greatly reduced. Victims may also become aware that they have become the victim of SIM swap fraud when they lose phone signal and so should be advised to contact their phone operator immediately if this occurs unexpectedly without regaining signal soon after.

While the increased use of two-factor authentication continues to help in the fight against online fraud, companies should be aware of the potential to exploit the frequently-used SMS second factor. Businesses should continue building layered strategies and using technology to identify suspicious account activity and fraud risk to avoid an over-reliance on SMS security codes in customer authentication.

Ubisoft

Sithy Phoutchanthavongsa, Ubisoft's fraud expert on the status of online gaming industry fraud, with insights into the grey market

About Sithy Phoutchanthavongsa: Sithy is the fraud expert at Ubisoft. He has 10 years of experience in fraud detection and prevention strategy performed within banking and ecommerce sectors, first as part of the business teams and then as a fraud service provider. He joined the Ubisoft ecommerce team in 2016. His mission is to define Ubisoft's fraud strategy and to dig out and respond to any risk related topics.

Sithy Phoutchanthavongsa | *Fraud expert* | Ubisoft

What are the main types of fraud in the online gaming industry and what transaction types are the most affected?

As the gaming industry becomes increasingly digital, it becomes exponentially exposed, especially at a transactional level. While the videogame consumer population is particularly aware of grey markets and tricks, fraudulent channels of retail are easy to put in place. Well-informed final customers just need to give the fraudster their player account credentials so the fraudster can process the transaction on their behalf with a stolen payment method.

All of these points make the fraud on gaming products attractive to fraudsters. Immediate consumable digital contents, like in-game currency, are the most popular products among fraudsters. In that case, it is not only about the financial impact, but this situation also brings inequity between players who can afford to buy extra content to be more competitive and those who can't or don't.

Given the international coverage, what insights can you share with us regarding fraud across different countries?

Because most of the defrauded products are digital content, the underground videogames market is global.

It is very important to be able to display a consistent product pricing list all over the world as well as it is important to be able to properly identify the customer's country. This way you will avoid customers from strong currency countries buying on softer currency countries.

In terms of fraud detection, the most important is to have a consistent payment method strategy for each geographical area. Then you should be aware of all the specificities related to the main payment methods. Is it easy to do a chargeback? What is required to open the payment account? How does the payer log in his account?

> *"The best tools for fraud detection would never be complete without both a good knowledge of players and a consistent external/customer communication.*

For example, 3-D Secure in Europe is reliable, while the chargeback process is easier in North America. Some countries tend to use payment methods that can be more trustworthy because they need more authentication clearances during the account creation process, or during the transaction step itself.

Take all of these specificities and build a tailored fraud strategy according to each area. →

What are the best fraud prevention strategies for securing both the online gaming platforms and the consumers' data? Is there any particular authentication method that you recommend?

During the real-time scoring, it is important to couple both a wide enough metrics panel and the knowledge you have on the player. We consider that whatever metrics say about the customer during the transaction, it always has to be contextualised by the data on players' habits, stats, history.

Reactivity is also key and has to be optimum; because digital transactions are instant delivery, it is important to put in place dynamic tools and rules that can be updated very quickly, such as with machine learning systems.

As for the player's data protection, Ubisoft takes the GDPR rules very seriously. We have a dedicated team in place to help apply it everywhere it is needed, every step of the way, and maintain our policy up to date.

When it comes to authentication, any type of two-factor authentication is recommended, whether by mobile or email. On top of regular transaction authentications, education is key. Providing players with all the necessary information to understand why and how to protect their account can help change their habits.

How are you dealing with false positives and false negatives? What challenges do you encounter in this matter?

Obviously, using relevant analytics tools and defining and monitoring the appropriate metrics helps. Yet, the importance of communication and collaboration with teams outside of the fraud department should not be underestimated: customer service or business operational teams can definitely help reduce false positives on the condition to build an efficient channel of knowledge sharing and information escalation. This is a great way to reduce friction generated by false judgement.

At Ubisoft, our main challenge is that, with over 14,000 employees located in more than 30 countries, we need to keep everybody on the same page and streamline feedback collection.

UBISOFT

About Ubisoft: Ubisoft is a leading creator, publisher, and distributor of interactive entertainment and services, with a rich portfolio of world-renowned brands, including Assassin's Creed, Just Dance, Tom Clancy's video game series, Rayman, Far Cry and Watch Dogs. The teams throughout Ubisoft's worldwide network of studios and business offices are committed to delivering original and memorable gaming experiences across all popular platforms, including consoles, mobile phones, tablets and PCs.

www.ubisoft.com

We encourage fraud prevention experts to share their knowledge with their peers in order to bring a positive impact on the online business environment. Therefore, what advice can you give to other merchants so they can keep their business secure and their customers loyal?

Ubisoft's ambition is to maintain a direct and active channel with players. The best tools for fraud detection would never be complete without both a good knowledge of players and a consistent external/customer communication. The benefits of fair play between players, the importance of securing their accounts, and not buying from unauthorised resellers, the reasons for limiting friendly fraud behaviors… All of the above should be brought to players' awareness in an educative and appropriate way. This combination is key for fraud mitigation success.

Richemont

With Low Order Volumes, Richemont Faces a Different Fraud Review Challenge

About Leon Brown: Leon Brown is the Fraud & Payments Manager for Richemont. Leon is managing the Fraud & Payments for all ecommerce Maisons, operating under the Richemont umbrella. With nearly ten years of experience in Fraud & Payments, Leon's previous experience includes Selfridges and Net-a-Porter.

Leon Brown | *Fraud & Payments Manager* | Richemont

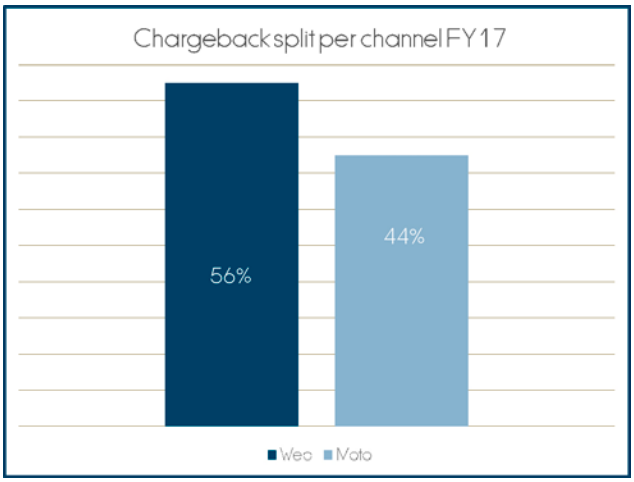
When implementing a fraud strategy for each Richemont brand, the key is to ensure we provide an efficient and seamless verification process. This rules out the possibility of using any verification method that may cause delay to the shipment's order or inconvenience to the client. As less than 30% of Richemont ecommerce orders are placed by returning clients, good customer service plays a crucial role in the way we handle orders placed predominantly by new clients.

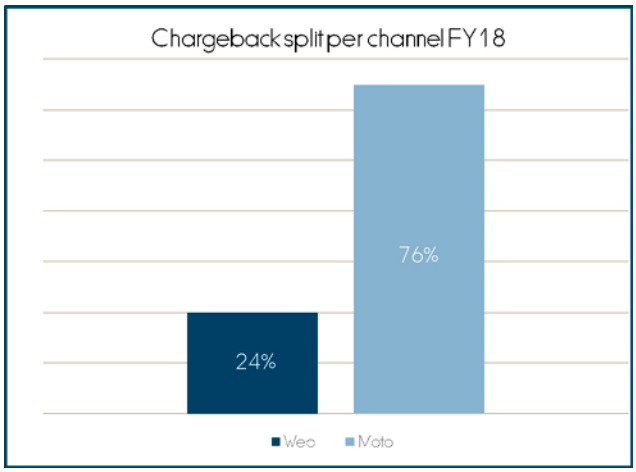
Fraud challenges at Richemont

As an online luxury retailer, we face many challenges with fraud management. At Richemont, we experience vast volumes of card testing fraud in Italy and France; in the UK, we see an emergence of 1st party fraud and account takeovers. However, our biggest challenge for the Richemont Fraud & Payments team is fraud on MOTO orders.

MOTO, an acronym for Mail Order/Telephone Order, represents 50% of the transaction split for Richemont. Due to the value of the products sold within Richemont brands, we find that the client usually prefers to speak to a brand specialist before deciding on the purchase. Unfortunately for us, the MOTO channel is also preferred by fraudsters.

Since we introduced 3-D Secure in 2017, we have seen a change in the fraudster's behaviour. As illustrated in the chargeback analysis, we have seen the fraudsters drastically shifting from targeting the websites to targeting the MOTO channel and placing an order via Customer Services. →





What is a MOTO order and why is it the preferred target of the fraudsters

Mail order telephone order is when clients decide to contact the Customer Relations centre, as they want to place an order over the phone, instead of using the website. There are several reasons for why this happens. The main reason is that many of our clients prefer the experience of speaking to a trained brand expert for reassurance before making such a huge investment. Another reason is that many of our clients may experience problems placing an order via the website due to the widespread issue we have with card issuers declining high-value transactions under the "do not honour" reason code. Once the client is put through to a brand specialist, their order is placed by the specialist using an internal version of the website. Once the order is complete, the client will receive confirmation of their order via email.

The reason a fraudster prefers to place an order via the MOTO channel is a simple one: lack of security.

On the website, we are protected by 3-D secure in most cases, and for the boutiques, we have chip & pin. For MOTO, we have none of the security features mentioned above. To place a MOTO order, you need an address, a card number, expiry date, and the CV2. In the UK, the US or Canada, we sometimes have the AVS for reassurance; but what happens when we have a high-value MOTO order from France or Italy, where AVS is exempt, with a billing and shipping address mismatch?

Rejecting an order, just because there is no AVS or because there is a mismatch with the billing and shipping, is not an option.

Dealing with the risk of MOTO at Richemont

Although 76% of chargebacks received is through the MOTO channel, the fraud and chargeback rate for Richemont is still comfortably below the acceptable industry average. Here are a few tips we use to manage fraud on MOTO orders.

Fraud tools. It's essential to research and invest in tools that can help you with order verification. In particular, invest in tools that can help you with address, email, and phone number verification. Since the implementation of several fraud tools, we have drastically reduced fraud in key markets like the UK.

RICHEMONT

About Richemont: Richemont owns several of the world's leading companies in the field of luxury goods, with particular strengths in jewellery, watches, and writing instruments. Our Maisons encompass several of the most prestigious names in the luxury industry including Cartier, Van Cleef & Arpels, IWC Schaffhausen, Jaeger-LeCoultre, Officine Panerai, Piaget, Vacheron Constantin, Montblanc, Alfred Dunhill, and Chloé.

www.richemont.com

Verification question. It's always tricky when you have to remember a lie. Based on our experience, this is usually the case with fraudsters. If we highly suspect a MOTO order, there is no harm in calling the client to verify a few order details. What we find in most fraud cases is a hesitance or reluctance to confirm certain aspects of the order. For example, the fraudster can verify the shipping address but struggles to confirm the billing address. It's crucial that you understand your typical client and use this as a benchmark when speaking to a potential fraudster to identify discrepancies in their behavior, the tone of voice.

Feedback. Speak to your Customer Service department and ask for feedback. How long did the client spend selecting the product, compared to your typical client? If the item he requested was out of stock, was the client specific with their back up option, or was the client just eager to complete the transaction?

mpe Merchant Payments Ecosystem

February 19-21, 2019 **Berlin**

REGISTER NOW TO SAVE 10%

Available until December 31

INDUSTRY LEADERS & INNOVATORS

150+ SPEAKERS

Want to hear & network with the industry's top minds about:

NEW APPROACHES IN FRAUD DETECTION & PREVENTION

Here are just a few you'll hear from

Rahul Pangam
CEO & Co-Founder
Simility

Martin Sweeney
CEO
Ravelin

Bartosz Skwarczek
CEO and Founder
G2A.com

Kelsey Blakely
Fraud Risk Operations Lead
Square

Steve Cook
Specialist Biometrics and Fintech Consultant
bioecom.com

Emilie Grunzweig
Head of Marketing Analyst
Riskified

Kieran Cotter
Fraud Risk Manager
Argos

... and many more to be revealed soon !

1000+ ATTENDEES

300+ C-LEVEL EXECS

150+ SPEAKERS

70+ SPONSORS & EXHIBITORS

300+ FINTECH PEERS

45 COUNTRIES

Visit **www.merchantpaymentsecosystem.com** for more information

Best Practices of Mitigating Fraud in Banking

Fraud Mitigation - Key Challenges for Banks

Mirela Ciobanu | *Senior Editor* | The Paypers

The financial services industry continues to position itself in a juggling position, with banks and financial services institutions facing multiple challenges tied to regulations, legacy systems, disruptive models and technologies, new competitors, and a highly demanding customer base, while pursuing new strategies for sustainable growth.

For 2018, banks have had to deal with managing their digital channels and threats associated with their use, such as new account opening and account takeover, implementing the Open Banking and Instant Payments initiatives, bringing to life the ultimate digital banking experience, adopting cloud services and data analytics, all frosted with the increased threat posed by fraudsters that are getting more and more sophisticated.

As the threat environment continues to escalate, effective fraud prevention has become an increasingly competitive issue for FIs. According to **a research conducted by iovation and Aite**, the most challenging fraud cases for FIs are sophisticated card fraud, application fraud, account takeover (ATO) attacks, wholesale ATO, and the spectre of faster payments.

Fraudsters getting more sophisticated

Despite efforts to control payments fraud, it appears financial institutions and businesses across the globe are fighting a losing battle. **A TransUnion study has revealed** that 94% of financial services have experienced fraud within the last two years, such as identity theft, synthetic identity fraud, or account takeover.

In addition, the European Payments Council (EPC) issues a yearly report on trends in security threats that affect the payments landscape. In **its most recent report, from December 2017**, the organisation identified the main payments threats, some of which we will try to cover briefly in our article:

- **a greater degree of professionalism of cybercriminals** shown by the organisation and sophistication of recent cyber-attacks;
- **the number of DDoS attacks is on the rise**, with bad actors frequently targeting the financial sector;
- the **attack focus has shifted from malware to social engineering attacks**;
- **botnets still remain a significant attack vector**, and because of the high volume of infected consumer devices (eg PCs, mobile devices, etc) severe threats remain;
- **mobile devices and IoT devices** are becoming **an attractive target** for cyber criminals;
- the **adoption of cloud services together with big data analytics technologies**, which results in data stored 'everywhere', are **bringing** new opportunities to businesses, but **new risks** as well.

The **financial services** industry has always been heavily regulated, and security and fraud prevention mechanisms are generally stronger than in other industries. Nevertheless, fraudsters see fintech providers as easier targets than traditional financial services companies as they attempt make use of new and emerging platforms to exploit gaps in process and infrastructure. ➔

Fraud Mitigation - Key Challenges for Banks

Some of the reasons behind this vulnerability could be that fintech companies do not necessarily have the resources such as skills and funds to implement sophisticated fraud defence/detection mechanism. **According to JAX Finance speaker** Rona Ruthen, fintechs are especially vulnerable, as in the early days the team is very lean, and the focus is on developing the product/systems and finding the product-market fit. Fraudsters know that, so they target fintech companies early on, and adapt very quickly to changes in controls.

Nevertheless, big financial services companies' customers are also targeted, despite having strong defences. One of the most effective ways of defrauding customers is to lure them into complex **social engineering** scams that result in a genuine customer unwittingly **transferring funds to a mule account**, or even allowing direct account access.

These attacks/attempts can take place across many channels, including email, SMS, calls, and social media channels, as any communication channel used to communicate with customers and users can be exploited by an attacker, with varying degrees of sophistication required to carry out the attack. All types of social engineering attacks continue to be used by attackers of varying levels of capabilities, with particular **increase in Business Email Compromise** emails and **phishing emails** that result in malware being deployed on computers.

To fight them, **financial institutions are advised to put the appropriate transaction filtering and monitoring systems** in place and **use customer profiling** to detect suspicious payment transactions. However, a very important aspect to counter the social engineering attacks is continued awareness raising campaigns.

Another big threat in financial services comes from **device spoofing**, as fraudsters attempt to trick banks into thinking that multiple fraudulent login attempts are coming from new customer devices, perhaps by repeatedly wiping cookies or using virtual machines.

Regarding the **mule accounts**, mule networks continue to negatively impact the global banking ecosystem, according to the **ThreatMetrix Q2 2018 Cybercrime Report**. **Money mules** are people who serve as intermediaries for criminals and criminal organisations. Whether or not they are aware of it, they transport fraudulently gained **money** to fraudsters. Thus, the use of intermediaries makes it difficult to figure out the identity of the fraudster. The challenge for financial institutions is how to detect mule activity when individual account behaviour may not trigger high-risk flags. To fight it, organisations need to create mule watchlists, and build machine learning models to identify new mule networks based on existing risk factors.

Offering the ultimate digital banking experience

Current onboarding processes are seen as time-consuming, costly, and as if they deliver a poor customer experience. However, when trying to innovate and offer great and frictionless customer journey while banking, financial services institutions are struggling to balance this experience with security threats. →

Fraud Mitigation - Key Challenges for Banks

Among these threats, on top of the list are **account takeover** and **new account applications**. Account takeover is a form of identity theft. This type of fraud doesn't necessarily have to start with what is traditionally considered highly sensitive information, such as a social security number or PIN. **According to Chargebacks 911**, account takeover can potentially be started from nearly any scrap of personal data: an email address, a full name, a date of birth – any identifier entered during the validation process can work. Historically speaking, banks and card providers have been the main targets of account takeover fraudsters.

Application fraud has become an increasing issue for organisations in industries such as banking, credit card applications, instant store credit, and retail, to name a few. **Some of the reasons behind the rise of this type of fraud** might be the large volume of personally identifiable information (PII) available on the black market for fraudsters to use, the abandonment of stringent manual application review processes by financial institutions and merchants when customers open new accounts, and fraudsters using stolen identity data combined with bots to open accounts at a very fast rate.

To prevent these types of fraud, financial institutions are advised to close the door on fraudsters before they can gain access to any account opening processes. InAuth security experts advise businesses to watch for bot attacks since they are capable of opening hundreds of accounts in a short amount of time, with bad actors often using the same device repeatedly to perform the fraudulent transaction until the device is detected and disabled.

Thus, **device authentication** is also an important way to thwart fraudulent account opening, as it enables organisations to verify the identity of a device by the device's unique characteristics. Moreover, a device riskiness assessment is needed to validate whether an additional review is necessary for the account opening process, such as bot detection, spoofing tool detection, malware detection, and the ability to use negative lists for devices associated to fraud.

Coping with Open Banking

Under PSD2 banks must open up their systems to authorised third-party financial service providers (TPPs) to enable these companies initiate and process payments and financial transactions at the request of the bank's customers. However, these requirements are a source of concern for many banks, as this access is not without risk. **According to OneSpan**, formerly Vasco, the most important security and privacy threats against the APIs provided by banks to TPPs include:

- API vulnerabilities, resulting in injection attack causing dump of personal information of bank's users;
- compromised or malicious TPP leaking financial information obtained from bank;
- API vulnerability leading to man-in-the-middle attack manipulating transaction data;
- compromised or malicious TPP issuing fraudulent transaction request;
- flooding of API affecting quality of service for users;
- compromised or malicious TPP locking out users with invalid authentication requests.

To overcome these threats, banks are advised to use transaction risk analysis to detect fraudulent transactions and user behaviour, choose a suitable authentication model for their users, protect the communication channel with TPPs, detect and prevent API implementation vulnerabilities and security incidents at TPPs. ➔

Fraud Mitigation - Key Challenges for Banks

Another key aspect in the context of Open Banking is consent that needs to be explicit, as mandated in PSD2 in accordance with the GDPR. Banks have to allow customer info to be shared, but only if that user explicitly gives permission to the new provider. However, third-party access to customer accounts and the associated data will inevitably raise concerns about security and privacy. **Consequently, privacy, consent, and fraud detection tools will become crucial to customer engagement and building in trust**.

As explained by Mike Nathan, ThreatMetrix, in the **Open Banking Report 2018**, banks must ensure the same level of security across all access points including the Open Banking environment, with the additional check around consent. They also must focus on risk control and put more emphasis on active risk management and monitoring.

Instant payments adoption

November 2017 saw **the launch of the SEPA Instant Credit Transfer (SCT Inst) scheme**, an initiative aimed at easier and faster payments on a pan-European scale. Among the features, the most relevant one is immediacy – when the funds are available in less than ten seconds after the transfer is initiated. One cannot omit benefits such as meeting the demand of customers for great payment experiences and replacing paper-based payment instruments, such as cash and cheques. However, this initiative has also left payments facilitators facing problems such as 'instant fraud', with banks having to adopt operational and risk management processes such as fraud detection to spot fraudulent transactions.

In this context, in the case of **authorised push payments fraud** it is hard to claim the amount of money back as funds are transferred instantly. And this is a rising concern; for instance the trade body UK Finance announced that businesses and consumers lost GBP 236 million in 2017 through authorised push payment (APP) frauds. APP frauds take place where a victim is conned into authorising a transfer of money from their bank account into an account, which they believe is controlled by a legitimate payee, but is actually controlled by a fraudster.

In order to avoid APP scams, educating consumers and business towards being more alert when making electronic money transfers is crucial. Internet users are advised to never disclose security details, such as their PIN or banking password, and should never assume an email, text, or phone call is authentic. Never rush a payment, as 'a genuine organisation won't mind waiting', **says the trade association**, which adds that 'listening to your instincts' and 'not panicking' are essential if something does go wrong.

Adoption of cloud services and data analytics

Cloud services are resources made available to users on demand via the Internet. They are offered by cloud computing provider servers as opposed to being provided by a company's on-premises servers. As organisations continue to migrate on-premises services and applications to the cloud, we can deduce that they will also suffer the same fraud threats and risk, with the addition of new ones. Weak code and software vulnerabilities in the cloud, outside the traditional perimeter of control, may produce **different types of breaches and fraud**.

To prevent these issues, the **European Payments Council (EPC) recommends** cloud providers to have a **clear set of policies** and cloud governance throughout the whole lifecycle of applications and services. Moreover, **the architecture, applications, process, systems, and data** in the cloud need to be **desegregated from each other to avoid propagation of malware or breach attacks**. →

Fraud Mitigation - Key Challenges for Banks

Last but not least, usage of new tools and applications for cloud computing and big data need to be analysed and assessed from the point of view of security, risk, and governance, as some tools might not be sufficiently mature to use and could potentially cause data breaches and fraud. Therefore, companies tapping into cloud services are advised to conduct a thorough analysis from the security and fraud perspective before making any usage or buy decision.

Conclusion

In our digital world driven by a mobile-first customer mentality, many financial institutions (FIs) have started to recognise and act towards satisfying the need for an omnichannel experience for their customers. But this task can became difficult as they need to determine with 99.99% accuracy the identity of the person on the other side of the computer or device, consider real-time fraud threats and real-time fraud solutions, while staying competitive and compliant. Fortunately, the digitization of banking services brings new technological solutions able to tackle modern security challenges and detect suspicious behaviour efficiently, helping financial institution services to protect digital data from fraud.

Feedzai

Machine Learning Innovations for Fighting Financial Crime in an Open Banking Era

About Pedro Bizarro: Pedro Bizarro is co-founder and Chief Science Officer at Feedzai. Pedro is a researcher turned entrepreneur: after a 10-year research career (Computer Science PhD at the University of Madison - Wisconsin, Fulbright Fellow, Marie Curie Fellow and winner of the BES Innovation National Competition) Pedro is now CSO at Feedzai where he leads the Research team in developing the best fraud prevention algorithms and tools. Pedro is a high performance data processing expert that loves data, algorithms, visualization, and machine learning.

Pedro Bizarro | *Co-founder and Chief Science Officer* | Feedzai

The fight against financial crime is changing and banks are struggling to keep up. Financial institutions are already losing ground in the adoption of open banking initiatives like PSD2. Coupled with the increasing market demands for compliance and transparency brought on by regulations like the GDPR, it's clear that banks have a lot to deal with. The financial industry is quickly shifting towards **real-time payments and instant services**, two key aspects of a frictionless customer experience. However, these frameworks present serious challenges to the security side of things – particularly where financial crime is concerned. At the same time, fraud schemes are growing more complex. For example, **according to Javelin**, "criminals are opening more new accounts as a means of compromising accounts consumers already have." And when it comes to money laundering, schemes now go beyond trafficking, with successfully laundered funds often being linked to bribery, influence peddling, corporate crime, or political intrigue. To protect their reputation and the trust they've built with their customers, banks need to look beyond their existing financial crime prevention strategies and discover how they can better address the world of real-time payments.

Three breakthroughs in fraud management

Over the last year, Feedzai has integrated three key features into its AI platform to help banks meet the growing challenge of real-time fraud prevention. Whether used separately or in tandem, these tools offer powerful new ways to stop fraud in its tracks.

OpenML

A primary drawback of many modern fraud detection systems is that they force users to operate within constructs that don't make sense for their enterprises. Until now, users were left with one of two choices:

- Work within inefficient data science environments offered by a vendor;
- Rely on their own (and often legacy) fraud management platforms that lack modern machine learning algorithms.

Feedzai understands that this is an impossible choice and offers a third door: Open Machine Learning (OpenML). Known colloquially as **"bring your own machine learning,"** Feedzai's OpenML Engine is a machine learning environment that lets users integrate their own machine learning tools, libraries, algorithms, and models into the system. In essence, it gives users access to a powerful fraud management platform while still allowing customization to the user's specific needs. The OpenML Engine includes an SDK for Python, R, and Java, while also providing close integration with machine learning tools like H20, R Studio, and DataRobot. It's a revolutionary integration that gives your fraud detection system the benefits of a purpose-built platform while letting you retain access to the open source libraries used by your own company. From a customizable fraud management perspective, there's nothing better.

AutoML

AutoML is Feedzai's way of accelerating the **machine learning process and increasing** the speed at which banks are able to confront new fraud threats. ➔

Before, users had to manually execute many steps of model development, including feature engineering, a very time consuming task. AutoML changes the game by providing a completely automated solution for model generation and development, all built into the Feedzai platform:

- Automatic feature engineering;
- Automatic model training;
- Automatic hyperparameter optimization;
- Automatic model selection.

Other AutoML platforms on the market (such as those offered by Google) require substantial GPU capacity that most organizations just don't have. Feedzai's approach works differently, relying on patent-pending, semantic-based automatic feature engineering which significantly cuts down the needed processing power. AutoML relies on a short and simple user-defined configuration of the semantics of each field which is then used to produce features automatically. Overall, this allows financial institutions to quickly iterate on many models and configurations very quickly with minimal processing power. For example, complete profiles can be built around a single card, including the number of declined transactions in a given time period, the distance between every transaction location, the time between consecutive transaction for each card user, and more. All of this is done through an automated framework that requires minimal input from the data scientist, reducing the classic data science workflow timeline from eight weeks to one day. Less time spent on model creation means more time spent on data analysis.

Genome

Feedzai Genome is a powerful visualization tool that provides a comprehensive, top-level view of transaction data. Where OpenML and AutoML advance Feedzai's data analysis capabilities, Genome brings a visual perspective to the connections between financial transactions. Using a virtualization engine, Genome displays the interconnected relationships between transactions and creates a simple way to identify patterns throughout each data set. Users can view the relationship between each transaction, view transaction clusters around specific cards or users, and trace the complete lifecycle of every transaction made—all within Feedzai's platform. This addition brings a new level of analysis to Feedzai's fraud detection capabilities. Images play into humans' natural ability to spot patterns in visual data, and by taking a visual approach to transaction review, users can instantly spot the same patterns that may take fraud analysts weeks to recognize. This goes beyond mere data analysis or risk scoring and creates a new type of fraud detection system:

- Offering deeper and more thorough assessments of the complete financial data set;
- Enabling more efficient risk assessment, including deep insight into the underlying relationships among each flagged transaction;
- Being purpose-built to fight financial crime and highlight suspicious fraud typologies.

A systemic view of instant payments fraud

These advancements speak to a growing trend in financial crime detection: the need for financial service providers to take a system-wide view of interaction. From the registration of each transaction to every customer touchpoint, true security comes from complete, end-to-end assessments. The world of instant payments is ripe with opportunity – yet if banks want to make the most of these new frameworks, they'll need to be prepared to handle the challenges that will inevitably come.

InAuth and Accertify

Accertify and InAuth: Fighting Fraudulent Account Opening

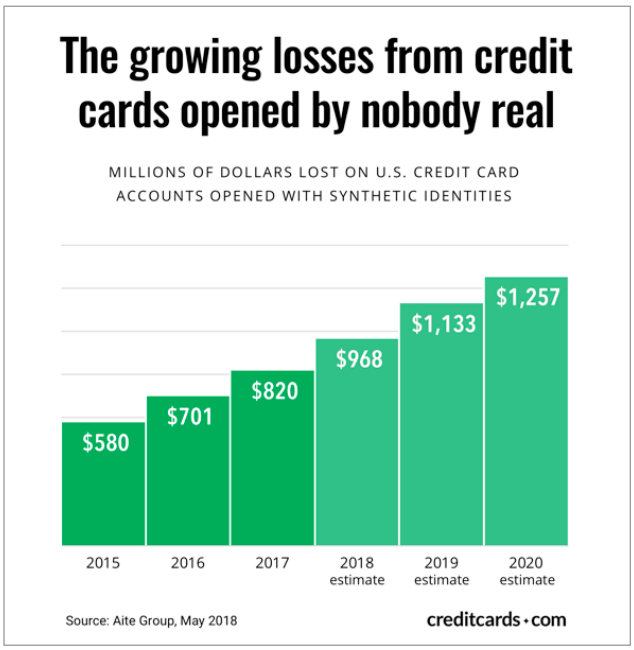
About Michael Lynch: Michael Lynch is InAuth's Chief Strategy Officer and is responsible for developing and leading the company's new products strategy, as well as developing key US and international partnerships. He brings two decades of experience in key roles within financial services, consulting, and Fortune 500 companies, specialising in security and technology leadership.

About Jeff Wixted : Jeff Wixted oversees the global operations, product strategy and roadmap, and presales functions at Accertify. Jeff brings over a decade of experience in cardnotpresent fraud and related use cases, he also serves as the Treasurer on the Merchant Risk Council Global Board.

Michael Lynch | *Chief Strategy Officer*
InAuth

Jeff Wixted | *Vice President of Product and Operations*
Accertify

Fraud takes place in many forms and in many industries, and has been rising in recent years. According to **PwC's Global Economic Crime and Fraud Survey 2018**, 49% of respondents said their companies had suffered fraud, up from 36% in 2016 – an increase driven by rising global awareness of fraud, a more robust response rate, and greater clarity around what 'fraud' actually means.



It is increasingly important to detect fraud at its earliest stage of the financial lifecycle, which, in many cases, is at the time of application for an account. Application fraud is a rapidly increasing issue for organisations in industries such as banking, mortgages, auto lending, financial lending, credit card applications, instant store credit, and retail, to name a few.

Credit card losses from accounts opened with fabricated identities reached USD 820 million in 2017, up almost 17% from 2016. In addition, **Aite forecasts** the losses to rise another 53%, to almost USD 1.3 billion, by 2020.

What can companies do to mitigate application fraud, particularly in digital channels?

The best way to prevent account opening fraud is to have robust protections in place across the customer lifecycle and to close the door on fraudsters before they can gain access to any account opening processes. Device authentication is an important part of thwarting fraudulent account opening, as it enables organisations to verify the identity of a device by the device's unique characteristics. Device authentication technology uses unique attributes in each device to create a device ID. →

By creating and calling on this device ID for subsequent transactions, organisations can authenticate trusted consumers with the least amount of friction, providing a positive customer experience. Transactions from risky devices can be flagged for next-level review or they can be denied altogether. If the same device ID is opening many accounts in a short amount of time, this is potentially a harmful bot. Another important tool in preventing application and account opening fraud is user behavioural analytics. By quickly recognising typical from atypical behaviours online, businesses can quickly identify potential fraud and prevent it before it becomes a loss. Cybercriminals today use bots to attempt to open several new accounts at once, by being able to tell the difference between a legitimate person attempting to open an account and a bot, which is critical.

Solution: an end-to-end risk platform to thwart account opening fraud

Accertify and InAuth are wholly owned subsidiaries of American Express and have been working with the largest brands in the world delivering fraud detection, with minimal customer insult so banks and merchants can prevent fraud while growing their business. By coupling InAuth's device intelligence with Accertify's risk engine, behavioural analytics and machine learning, businesses have unparalleled insights to thousands of device and transaction attributes – across all channels – to assess the riskiness of an application and make a truly informed decision. InAuth performs critical checks that could indicate that a fraudster may be working behind the scenes and helps validate whether additional review is necessary in the account opening process, such as bot and malware detection, along with the ability to use negative lists for devices associated to fraud. InAuth allows clients to associate device elements with anonymised user data across multiple industries, providing a holistic view of the trustworthiness of a device, so that they can better assess the riskiness of a transaction and take additional steps to mitigate potential fraud. In situations such as new account opening, any risk intelligence of the device itself becomes critically important in order to make more confident transaction decisions. InAuth provides critical context, allowing businesses to expand their real-time defence network and provide another layer of transparent authentication that can be seamlessly incorporated into the account opening process. Accertify's portfolio of fraud management solutions brings additional levels of control to identify and prevent account takeovers and new account originations schemes.

InAuth Accertify

About InAuth and Accertify: InAuth delivers device identification, risk detection, and analysis capabilities possible to help organisations limit risk, remove friction, and reduce fraud within their digital channels. Accertify, a wholly-owned subsidiary of American Express, is a leading provider of fraud prevention, chargeback management, and payment gateway solutions to merchants' customers spanning diverse industries worldwide.

www.inauth.com
www.accertify.com

Click here for the company profile

By looking beyond the user-entered information and examining anonymised site navigation data, customers are able to quickly identify and stop complex fraud attacks such as identity theft, bot traffic, and automated attacks that might be missed by other solutions. These behavioural analytics tools look at the speed and manner in which customers interact with websites when they complete their applications and establish usage patterns of legitimate customers vs fraudsters.

Accertify's solutions collect, store, and aggregate large volumes of data in real time. Creating views around a customer, a product, an event, or any number of data points can increase fraud detection accuracy and reduce false positives. There is no shortage of fraud prevention solutions on the market but it is important to partner with those proven to deliver results. InAuth and Accertify work with the largest global banks, merchants, and airlines and help turn large volumes of disparate data into actionable intelligence to help thwart online account opening fraud while protecting the user experience.

Nordea

The fraud management team of Nordea reveals key insights into the cybercrime trends and fraud management solution at both local and global level.

What are the current cybercrime trends in the retail and corporate banking sector, particularly in the Nordic countries?

We have divided cybercrime trends into local and global threats. If we are looking at the global threats, which are likely to rise in the coming year, we see investment scams, CEO fraud, Business Email Compromise (BEC) fraud, phishing, smishing, and vishing. Notably, vishing is prevalent in Sweden and it is likely to come to Norway and other Nordic countries. At the local level, the common threats identified are friendly fraud, identity theft, card scams, and again phishing. Nevertheless, the employees are usually the weak link, as in most cases the threat comes from the inside. Why? Because the staff within the organisation is not well trained to recognise a cyber-attack, or sometimes they commit fraud on purpose. Due to the developed economy and prosperous businesses, Nordic countries are highly digital, and this makes them a good target for cybercriminals.

How does the anatomy of cyber-attacks look like?

There are two types of cyber-attacks; however, it is often some kind of combination of the two: those where the fraudsters manipulate people's minds and those where the fraudsters manipulate people's devices (or hack/misuse email box, inlogging, etc). The first type is essentially the social engineering fraud and it is usually exercised over an organisation's staff. Cybercriminals hack emails, but most of the time, at least for CEO fraud, the manipulation of the employees is a common practice. The attacks that go through social engineering are investment scams, BEC fraud, love scams, phishing, smishing, vishing, friendly fraud, and identity theft, but they can also include bits of technical fraud.

The technical advanced fraud is when fraudsters have the skills and knowledge of producing technical bits in order to attack, so then they use malwares, different types of Trojans and viruses in order to get into the computers of the customers. By any means, the most successful frauds are those resulted from a combination of social engineering and technical elements.

Could you please share with our readers some recommendations on strengthening the fraud prevention management?

One of the important things to do, as an organisation, is to identify the risk group within. It's not always about the money, the information, or the different knowledge that only the company has; the projects or any other type or valuable resources that can be stolen and commercialised by fraudsters are also things worth considering. It is also important to know what information is shared between the company, the staff, and the public. In addition, one has to always make sure that the employees are aware of the risks, and they should always be updated about potential attacks. Therefore, educating people on a constant basis is a way of reducing risks. One should constantly monitor the way emails are used (for instance, how the flags in the email function are used), the money transfers, and other types of transactions.

> *"By any means, the most successful frauds are those resulted from a combination of social engineering and technical elements.*

When it comes to transactions, we recommend the four eyes principle: two people to verify when the company made a payment and to make sure fraudsters don't manipulate the bills or the emails. In addition, it's always crucial to make sure the utilised technology is up to date. And there is also the password culture: obviously, people should understand they shouldn't share passwords under any circumstances, and they should know how to build a strong password. Moreover, companies should adapt a correct password culture for their staff. →

Nordea

About Nordea: Nordea is the largest bank by size in the Nordic region and the only bank that has a truly Nordic identity at its heart and culture. With key operations in every Nordic country, Nordea has been playing a fundamental part in establishing the shared economy in the region and in fostering a borderless trading area.

www.nordea.com

Online Authentication - The Journey from Passwords and Secret Questions to Zero Factor Authentication

An Introduction to Online Authentication and Stronger Authentication

Mirela Ciobanu | *Senior Editor* | The Paypers

Traditionally, identity verification was based on human interactions and presenting physical documents, mainly issued by governments. Still, as digital channels are becoming the go-to places where consumers interact with businesses and each other, we cannot rely anymore only on those processes.

As a result, businesses have become incredibly dependent on technology to verify and authenticate identities in order to give (new) customer access to a network of systems to manage, store, and transmit information such as financial accounts, personally identifiable information, intellectual property, transaction records, etc. Within this web, identity verification, identity validation and identity authentication verification have turned out to be central to the ability of these businesses to effectively secure access to consumer-facing digital channels and the systems that underpin their operations.

However, **identity verification, identity validation and identity authentication** represent three different types of checks/digital transactions. **As Trulioo mentions in a blog** post, we need to build the necessary online framework of trust that can confirm that the person actually exists, by checking the validity of the identity data they provide and verifying that data.

The differences between the three cases mentioned above causes confusion as each involves different information and has different legal ramifications and requirements. While authentication is demonstrating ownership and control of a unique feature connected to an identity over time, identity verification and validation check if the information represents real data and aim to prove that the specified identity attributes are actually connected to a person, entity, or thing that they are intended to represent.

Strong Customer Authentication

In this chapter, we will be focusing more on explaining authentication and addressing strong customer authentication. This regulation will **apply to online payments within the European Economic Area (EEA)** where the cardholder's bank and the business's payment provider are both in the EEA. *However, some businesses outside of Europe may also be impacted depending on how European issuers implement the new authentication rules*.

The SCA requirement is **applicable to all electronic payment transactions** that do not benefit from an exemption and is **based on an authentication using two or more elements**. The elements are categorised as knowledge (something that only the user knows, e.g., a password, answers to personal questions, PIN), possession (e.g., something that only the user possesses, e.g. a debit card or mobile device), and inherence (something that user is, e.g., fingerprints). The **elements used must be independent from each other**, and the two elements used for an authentication must belong to different categories. ➔

An Introduction to Online Authentication and Stronger Authentication

Nevertheless, **for certain transactions**, the regulation also introduces **exemptions to the SCA requirement**. In brief, the RTS exempts contactless payments at point of sale under EUR 50, low value (online) transactions under EUR 30, transactions with trusted, pre-defined beneficiaries, subsequent recurring transactions, and low risk remote transactions subject to certain conditions. According to Irena Dajkovic, a partner of DALIR law firm, **other exemptions with more limited application scope include** those relating to transactions initiated by a legal entity (not consumer) through the use of dedicated payment processes or protocols and subject to regulator's approval, as well as those relating to access to certain information (balance and/or payment transactions executed).

Transactions that do not meet these new authentication requirements or qualify for any exemption may be declined starting September 14, 2019. However, **according to some PSPs**, **3-D Secure 2**, the new version of 3-D Secure rolling out in 2019, **has the potential to become the primary authentication method used to meet SCA requirements for card payments**.

Why do we need strong authentication?

- **To counterbalance the effects of multiple data breaches and protect customers against malicious actors** – For instance, in 2016, a **third of US businesses have had customer information breached** — including the information businesses rely on to authenticate their customers. The mass compromise of passwords has led to an increased risk of fraud on consumer accounts and network-level attacks from credential-stuffing botnet attacks.
- **To minimise false positives** (benefits for businesses: increase revenue by avoiding pushing good customers away) – As accuracy and customer loyalty are crucial for businesses, to win customer's support, authentication solutions must prove their effectiveness in both keeping bad actors out and ensuring a positive security perception for good ones.
- **Because we have the technology** - Mobile devices are a clear driver of traditional strong authentication. These devices have increased the opportunity for businesses to leverage more than just passwords to authenticate their customers and employees by facilitating both possession-based authentication (e.g., device fingerprinting, SMS-based one-time passwords (OTP), etc.) and inherence-based authentication (e.g., fingerprint scanning, voice recognition, etc.).

Strategies to bolster authentication

Cyber-criminals can be incredibly creative and determined when it comes to gaining access to consumer's accounts or enterprise's data. To fight these actors, **a number of tactics and strategies** to bolster authentication have been developed/presented by the private industry and public sector, including:

- **Risk-based authentication** – implementing authentication based on the degree of risk. Input data is analysed to determine which type of authentication is best to leverage following a determined degree of risk in a given transaction or interaction.
- **Continuous authentication** – a variation of risk-based authentication. In this case, user's actions through and across sessions are taken into account when deciding the degree of access he/she has, or whether certain types of authentication are needed.
- **Out-of-band authentication** – uses a communication mechanism that is not directly associated with the device being used to access the banking application or ecommerce site in order to facilitate a second mode of communication. Thus, it can mitigate the risk that exists when the initiating channel is compromised or simply too insecure for the level of risk in the transaction. →

An Introduction to Online Authentication and Stronger Authentication

According to Simility, a complex authentication process looks at various types of data, such as login, historical, cross-channel, behaviour, device, geolocation, etc. to effectively and seamlessly decision the end user. Users are automatically accepted, rejected, or required to step-up, such as in the case of high-risk transactions.

Also, the ability to tailor the authentication experience to the consumer's comfort zone is important since this increases the potential that the transaction will be completed, rather than abandoned.

Technology to the rescue

Financial services, banks, and merchants have different demands when it comes to users' authentication, and some factors and solutions are more vulnerable than others. Take for instance a password, PIN, and passcode which are vulnerable to interception or theft and replayed, or guessed versus facial recognition which is vulnerable to theft and emulation.

Facing the **demands of the market and regulators**, and at the same time **seeking to repel attackers**, those responsible for **choosing and implementing customer authentication face a herculean task. However, technologies such as machine learning and AI and, of course, biometrics can help businesses fight the bad guys**.

AI can evaluate a certain transaction, such as a log-in event, a shopping transaction, or a new-product application, by using its unique contextual and transaction data, and come up with a fine-grain decision about its implied or inherent risk. But, to be effective across geographies, analytics need a good consortium dataset and large pools of globally diverse risk and fraud data to draw on.

But there's a common misconception that this data invades privacy, which is not always the case. Vendors such as CA Technologies anonymise all the data they use for predictive modelling to ensure that consumer privacy is protected. It is the patterns of use over time that are important, and the profiles that accumulate these patterns cannot be tied back to an individual.

Another praised technology, successfully implemented by banks and other financial services companies to keep their customers safe, is **biometrics**. Their ability to perform without dependency on the user remembering or sharing a password greatly enhances customer security while improving the user's authentication experience. This technology includes device fingerprinting, behaviometrics, fingerprint scanning, eye scanning, facial recognition, and voice recognition; however, we will focus more on behaviour biometrics. →

An Introduction to Online Authentication and Stronger Authentication

Behavioural biometrics, sometimes known as passive biometrics, analyses how the user interacts with a device or session. There are some 2,000 parameters that behavioural biometrics depends on and they give a clear indication of someone's unique identity. These range from monitoring human motion gestures and patterns to keystroke dynamics and factors – such as speed, flow, touch, sensitive pressure, and even signature formats. Behavioral pattern detection technologies identify fraud by monitoring the user session to detect suspicious activities or patterns.

These anomalies manifest in a couple of ways:

- **Transactional:** The user is performing transactions that are out-of-pattern compared with normal behavior.
- **Navigational:** The manner in which the user is navigating the website is inconsistent with his or her usual pattern, is inconsistent with the pattern of his or her peer group, or is indicative of the navigational pattern of a bot.

Even though biometrics represent a desirable alternative to passwords, a simple replacement of passwords with stand-alone biometrics is generally not recommended. Such implementations would be comparably vulnerable to compromises under realistic threat models. Integrated solutions such as *multi-factor* and *multi-layer* should be adopted ***as acknowledged by 67% of industry professionals*** *in a Mastercard and the Department of Computer Science at the University of Oxford survey)*. Multi-factor approaches require users to respond to two or more explicit authentication challenges (e.g., multi-modal biometrics). Multi-layer approaches combine a single explicit factor with other data element that are typically invisible to users (e.g., device fingerprinting, geofencing, risk scoring).

Going further, when processing higher risk transactions, a number of biometrics can be combined in a step-up process called multimodal biometrics. This happens in order to prove someone's identity, known as Strong Customer Authentication. Even more, if the customer uses their fingerprint, face, or PIN code to unlock their device, banks can now pair that same user verification method with strong cryptographic protocols made available through on-device platform APIs, to allow customers to securely access their accounts online in full compliance with PSD2 strong customer authentication requirements, on both apps and websites.

Still, **no single method of authentication will always be suited for every situation**. Companies are advised to adopt approaches that use multifactor authentication, while also taking into account location, behaviour analytics, and numerous other indicators of identity.

ThreatMetrix

Reimagining Identity in the Post-Data Breach Era

About Alisdair Faulkner : Alisdair Faulkner leads the commercial markets and strategy function for fraud and identity management at LexisNexis Risk Solutions, Business Services. He was co-founder and Chief Products Officer for ThreatMetrix culminating in the 2018 acquisition by LexisNexis Risk Solutions. He now oversees the combined fraud and identity solutions for LexisNexis Risk Solutions and the ThreatMetrix Digital Identity Network.

Alisdair Faulkner | *Chief Identity Officer* | LexisNexis Risk Solutions

Data breaches have become commonplace among global headlines and newsfeeds, a painful fact of life until you become a victim yourself, and realise the wholescale devastation breached identity data can reap on your day-to-day life. The onus is squarely on businesses to ensure they have the appropriate defences in place to protect their customers, as well as safeguard their own reputation.

However, keeping personal data safe has become increasingly challenging for businesses, who must contend with the evolving demands of the digital economy amid ever more savvy, global cybercriminals. Businesses are tasked with having to stay one step ahead of the fraudster, no easy task when cybercriminals are launching increasingly sophisticated and organised attacks, using near-perfect identities created from piecing together breached credentials so readily available on the Dark Web.

The intrinsic link between stolen identity data and attacks is clearly evident through analysis of the ThreatMetrix Identity Abuse Index. With the largest spikes in the index associated with the biggest breaches reported in the news, the Index is a clear indicator of how the exploitation of stolen identity information is impacting the size and scale of global attacks. These volatile attacks are deployed to give cybercriminals access to everything they need in order to turn a profit with stolen credentials. Whether it be opening fraudulent new accounts, taking over existing ones, applying for fraudulent loans, making illegal payments or going on illicit shopping sprees, fraudsters are not only making a monetary impact on the businesses they target, but also threatening brand, reputation, and customer loyalty. Perhaps the clearest indicator of the impact of breached identity data is the fact that around one in ten new account creations in the ThreatMetrix Network is fraudulent, and for some industries this figure can be even higher. ➔

Thus, identity has become central when talking about success in the digital economy. In a post-data breach era, businesses must strive to re-establish trust online and gain insight into the true identity of customers.

However, with consumers moving seamlessly between their offline and online personas, across both their corporate and personal lives, businesses are faced with a myriad of challenges in ascertaining the true identity of transacting users. Muddying the waters further is the fact that individuals can behave differently and show different offline personas depending on the circumstances, for example, subscribing for media services online versus applying for a business loan.

Traditional fraud and identity management is failing to keep pace with this evolving fraud landscape – siloed and disjointed technologies built to defend against various threat vectors introduce unnecessary friction for the user, at excessive cost to the enterprise. Different ways of assessing users at different customer touchpoints often means asking customers to jump through multiple hoops to prove who they are – again adding friction to the overall user experience.

Businesses can meet these competing priorities – protecting against fraud while providing a frictionless user experience – by having a complete 360-degree understanding of who they are transacting with – anywhere, anytime, and via any channel.

But how can this be achieved? The secret to success is linking the multi-faceted parts of an individual's true identity in a way that is actionable across multiple channels. The ability to join the dots between a person's offline and online identity requires access to the most comprehensive sets of data and sophisticated technology to create and analyse linkages to form actionable intelligence that can be used in real time.

1. **Digital Assessment:** To gain a truly 360-degree view of identity, businesses should incorporate identity attributes seen during digital touchpoints such as username and passwords, email addresses, online account history and behaviours, social networks, device identification, and geo-location.
2. **Identity Verification:** Involves linking attributes of an individual's digital identity to authoritative data sources from a person's offline records. This includes identity verification based on utility bills, car registrations, and government-issued identifiers such as social security numbers.
3. **Analyse Fraud Risk:** Advanced linking technologies and machine learning can then correlate these disparate data points and turn this into actionable intelligence on risk through fraud scores and reason codes; determining velocities and frequencies that are indicative of trusted versus suspicious behaviour.
4. **Step-Up Authentication:** For activity that shows elevated risk analysis the final step is deploying step-up authentication, for example knowledge-based authentication, secure notifications, or biometrics. Strong customer authentication that integrates seamlessly with risk-based authentication, based on identity assessments, is key to delivering maximum security with minimal customer intervention.

The combined understanding of physical and digital identity interactions allows businesses to respond quickly and more comprehensively to the vast number of threats facing the global economy. Solving the problem of identity in the digital age will enable a seamless and comprehensive approach to fraud and identity risk management to help companies drive online revenues by making faster decisions, reducing online fraud and combating emerging threats.

RSA

Adaptive Authentication: Balance Opportunity and Risk in an Omnichannel World

About Mathew Long: Mathew Long is a Sr. Advisor for the RSA Fraud and Risk Intelligence division. Mathew leads the global go-to-market efforts for RSA's consumer authentication and fraud intelligence solutions. Mathew is a prolific blogger and a regular presenter at industry events and media engagements. For the past six years, he has focused on working with leading financial institutions on anti-fraud and cybercrime prevention strategies to reduce fraud and improve customer experience.

Mathew Long | *Senior Advisor, Fraud & Risk Intelligence* | RSA

The age of digital transformation has arrived, revolutionising the financial services industry with new ways of doing business anytime, anywhere. With a growing array of digital banking channels available, customers seemingly have infinite possibilities for conducting financial business. At the same time, this expansion of banking channels increases the risk of fraud.

Winning in the digital era means rising to the challenge of meeting an entirely new set of customer expectations. As Hari Gopalkrishnan, CIO of Client Facing Platforms at Bank of America put it, 'Our customers don't benchmark us against banks. They benchmark us against Uber and Amazon.' To succeed, FIs must manage digital risk so that it doesn't stand in the way of digital opportunity. In the middle of the fulcrum sits customer experience.

Top five areas for digital opportunity

There are five key areas of digital opportunity for the financial services industry, as follows:

Fintech

Fintech is transforming the industry. Digital wallets, cryptocurrency, blockchain, and other Fintech offerings are redefining banking and financial services in a multitude of ways, putting traditional FIs at risk of losing business to them. Increasingly, traditional banks are rapidly innovating to provide more of the kinds of digital services their Fintech competitors offer.

API economy and Open Banking

The API economy offers customers the option of convenience such as being able to link their accounts with other services (utility payments, for example) without the FI having to build out a complex technology infrastructure to support the new capability. In some cases, this may be more than an opportunity; it may be an obligation. For example, the European Union's (EU's) Payment Services Directive II (PSD2) requires banks doing business in the EU to open access to their systems to payment services and data aggregators.

3-D Secure 2.0

Card issuers and issuing processors have started or are planning to embark on the journey of adopting EMV 3-D Secure (AKA 3-D Secure 2.0). The opportunity for 3-D Secure 2.0 lies in its adoption of consumer-friendly features such as the elimination of enrolment pop-ups, full integration into the shopping experience, and faster authentication. By reducing the annoyance factor, these changes have the potential to lead to more approved transactions and more revenue.

Mobile banking

Mobile banking has become a staple of consumer offerings. In fact, the mobile channel has become the predominant and preferred channel for consumers. →

According to RSA's Quarterly Fraud Report, in the last three years, transactions from mobile apps have increased over 200%, and the overall volume of activity in the channel now outpaces that of the web with 55% of all transactions conducted from a mobile app or mobile browser. As a result, FIs are expanding their mobile channel to provide new services to their customers while meeting their demands for secure, convenient account access.

Internet of Things (IoT)

While banking does not lead the list of today's top IoT applications, the prospects for IoT-based financial transactions look good nevertheless – particularly in the payments segment. IoT is an emerging area, deemed the next evolution in banking and shopping convenience. The concept of 'human-not-present' transactions where IoT devices interact directly with payment systems is not far off and it will enable more personalised services, facilitate usage-based fees, and much more.

Stop fraud, not customers

As the array of digital channels grows, so does the need for security technology that can detect and prevent fraud in ways that are frictionless for customers. Adaptive authentication solutions leverage machine learning models to assess fraud risk based on contextual information such as device identification, IP address, user behaviour, and fraud intelligence (eg mule accounts). Its nonintrusive nature, flexibility, and ability to manage fraud risk across multiple channels makes adaptive authentication an ideal solution for FIs looking to deploy strong security to large customer populations.

Adaptive authentication technology can achieve fraud detection rates of 95% with minimal customer intervention and it allows for integration with numerous step-up authentication methods in the event of a high-risk scenario, including out of band SMS or email, biometrics, transaction signing, and more.

With so many channels for customers to interact, omnichannel fraud detection has become a hallmark of adaptive authentication. Back when 'multiple channels' at most meant a branch bank and an ATM network, this wasn't so much an issue.

RSA

About RSA: RSA, a Dell Technologies business, offers business-driven security solutions that uniquely link business context with security incidents to help organisations manage digital risk and protect what matters most. RSA's award-winning cybersecurity solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high-risk world.

www.rsa.com

But today's banking channels are also likely to include online banking, chat support, mobile banking, call centre, IVR, and third-party services, with more channels, such as IoT devices, on the way. In this environment, siloed operations are both ineffective and unsustainable.

Adaptive authentication allows operations to be carried out as a whole rather than an array of discrete parts. This eliminates the need to build and maintain a separate infrastructure (including separate point solutions for fraud detection and prevention) for every channel. Instead, all channels – both online and offline – can share knowledge and awareness of a customer's interactions and lead to streamlined operations, a more secure banking environment, and a smoother customer experience.

HID Global

The Paypers interviewed Olivier Thirion de Briel, Global Solution Marketing Director at HID Global, about what role authentication plays within the Open Banking ecosystem. Following are takeaways from our discussion.

About Olivier Thirion de Briel: Olivier Thirion de Briel is Global Solution Marketing Director for the banking sector at HID Global. In this role, Olivier leads the banking strategy and product marketing for the IAM solutions business unit. Prior to joining HID Global, Olivier led the cloud strong authentication offering at OneSpan (former Vasco) and the Oberthur Technology's strong authentication product line. Olivier holds an MBA from INSEAD, as well as an MSc in computer and electronic science.

Olivier Thirion de Briel | *Global Solution Marketing Director* | HID Global

Rules have now come into effect, requiring banks to share their customers' financial information with other authorised providers using open Application Programming Interfaces (APIs). However, this makes banks dependent on the security of the Third Party Providers (TPPs) using these APIs. What are the possible risks of this new Open Banking era?

Under the Open Banking initiative, institutions must open their APIs to give TPPs access to their customer data. In other words, if a bank's customers want to use one of these TPPs, the bank must give the TPP access to its stored data about them and allow the TPP to serve these customers via the open communication interface.

Open Banking benefits financial institutions by enabling them to build new business models around a variety of innovative and more personalised customer services. But it also exposes a bank's customers to a greater risk of fraud since their financial data must now be shared with multiple TPPs. The problem is not so much that the data is being shared through Open APIs, but that it might be shared without properly authenticating both the TPP and user.

In this context, I would like to emphasise two points that will play a critical role in the future. First, banks must prevent data loss, identity theft and non-compliance with data protection regulations by using identity verification and fraud prevention solutions that ensure personal data is shared only with the consent of its genuine owner. Second, banks will need to ensure that each TPP is known, trusted, and has strong enough security policies in place to safeguard all shared data.

Strong customer authentication is especially important and must be the central element in the Open Banking API ecosystem. It must be a priority both for banks, which already understand that sensitive data requires high security and protection, as well as for TPPs, which are only at the beginning of their learning curve.

> *"As financial fraud incidents grow in digital banking channels it is imperative that institutions protect their customers.*

What security measures should banks adopt to address these threats and challenges?

Banks have come to realise that they will be the central point of authentication in this growing financial ecosystem. When data must be shared with a TPP, the bank is in the best position to deliver a seamless authentication experience that does not compromise security. Customers will not tolerate an authentication experience that meets security requirements at the expense of convenience. They have come to expect easy, on-the-go online access and mobile transactions and will not accept time-consuming processes in this emerging Open Banking ecosystem. →

Different authentication models have their own characteristics and security implications. Can you please describe the ideal authentication process?

In this new digital era, the authentication process must be based on an adaptive security approach in which the level of complexity depends on the risk associated with the transaction. This risk level is established based on multiple parameters including malware detection, geolocation, IP address, and how the customer is using a mouse or keyboard or displaying other behaviours. Some solutions can evaluate a transaction's risk level based on characteristics of the user device and its browser and other attributes.

If the risk level based on these parameters is defined as low, authentication may only require a username and password. If it is defined as high because the transaction is being conducted with an unknown beneficiary at an unusual place and time, additional authentication methods may be required to prove the user is who he or she claims to be.

It is also important to understand that growing use of connected devices has expanded the attack surface for financial fraudsters. Risk-based advanced authentication will need to take into account the entire environment in which customers are transacting to provide the necessary protection.

Since PSD2 allows third party providers to access customers' payment account data, in what way is this directive aligned with GDPR? How will discussions about data analytics evolve over the next 5 years?

Open banking is about sharing data and making it available to TPPs. GDPR, on the other hand, aims to ensure that nobody can steal personal data. In fact, the goals of GDPR, Open Banking and PSD2 are all aligned around giving data ownership back to users. This is where security plays a key role, and GDPR brings an additional layer of requirements for securing sensitive data.

Machine learning and AI will enable banks to collect and analyse data so they can make smarter real-time decisions about the next action to take when a threat is detected, including whether to approve, block or reject a transaction. Adaptive authentication processes will enable them to define security levels based on existing risk.

About HID Global: HID Global is the leading provider of trusted identity and access solutions for people, places and things. We enable organizations and enterprises in a variety of industries such as banking, healthcare, and government to protect digital identities in a connected world and assess cyber-risk in real-time to deliver trusted transactions while empowering smart decision-making. Our extensive portfolio offers secure, convenient access to on-line services and applications and helps organizations to meet growing regulatory requirements while going beyond just simple compliance.

www.hidglobal.com

Click here for the company profile

As these technologies are brought to the Open Banking API ecosystem, we will also see financial transactions based on connected devices. Within this ecosystem, the use of static multi-factor authentication methods will decrease and we will see a migration to continuous data analysis that improves risk-mitigation decision-making and creates a more secure transaction environment.

Arvato Financial Solutions

Seamless and Secure Online Authentication: A Solvable Goal?

About Robert Holm: Robert Holm is Senior Vice President Fraud Management at Arvato Financial Solutions. With an experience of almost 20 years in setting up and growing new businesses, he leads the strategic development and internationalisation of the fraud management division.

Robert Holm | *Senior Vice President Fraud Management* | Arvato Financial Solutions

Online authentication is an intelligent tool that allows companies to differentiate legitimate activity from fraudulent behaviour to make sure only the right users get through. However, as intelligent as it may be, there does still remain a challenge in making sure the wrong users with the right credentials don't cheat their way past this barrier. This means that no company can ever really be 100% sure about the true identity behind an online user.

Approximately 98% of human transactions are legitimate, meaning only 2% are fraudulent. With such favourable odds, one would think it was a given that businesses shouldn't be quick to treat all customers as potential fraudsters. But some do. And in doing so, instead of protecting their business, they end up pushing loyal customers away. We could conclude that overly strict defence mechanisms won't let all legitimate customers through. On the other hand, interruptive authentication methods cause transaction abandonment and loss of customers.

Fraudsters continue to find ways to overcome traditional authentication methods, as we have grown accustomed from them to do so. Static defence mechanisms do not prevent all cases of fraud: login data is being bought on the dark web, CAPTCHA is being outsmarted by bots, true geolocation is being hidden via proxy servers, device fingerprinting is being imitated by emulators, and multi-factor authentication is being surpassed when session takeover occurs. That's why the industry has been forced to think beyond passwords and secret questions, and research advanced authentication methods.

As unique as a fingerprint

The way we subconsciously behave on our phones or computers – how we hold, scroll, swipe, click, tap, or type – is as unique as our fingerprints.

By using sensors in touchscreens or codes on websites, data can be collected invisibly to the user. Multiple interactive gestures can be constantly analysed — including how the person is holding the device or the speed and rhythm in which they're using their mouse. Endless amounts of these data points together form a digital fingerprint and can be used to establish a user's identity.

> *"Until passive behavioural biometrics, online fraudsters had a method for overcoming the security of traditional authentication methods.*

With the aid of these behavioural biometrics, companies will not only be able to accurately differentiate between legitimate customers, fraudsters and non-human behaviour (eg BOTS, malware, or Random Access Trojans), but they will also save costs with fewer suspicious cases to check manually. ➔

And it can do more than reducing fraud threats and financial losses. Companies are also able to minimise false positives and increase revenue by avoiding pushing good customers away. Additionally, leveraging the user's behavioural biometric data means businesses receive additional valuable insights about their customers. This allows for further optimisation of the customer journey and user experience – improving customer loyalty and encouraging higher conversion. In fact, **Gartner states** that by 2022 digital businesses with a great customer experience during identity corroboration will earn 20% more revenue.

The great advantage of this new authentication method is that even if fraudsters try to use stolen passwords and other personal information, behavioural biometric monitored accounts can still be secured, as this type of information can't be stolen, faked, or copied.

Behavioural biometrics differentiators

In contrast to other protection methods, such as active physical biometrics, there are many positives when it comes to passive behavioural biometrics:

- It does not depend on special scanning hardware and is independent from devices or locations.
- Authentication is not one-time validation, but a continuous process from check-in to check-out – protecting transactions including registrations, purchases, payments, and money transfers.
- No extra user actions are required. It is frictionless and seamless and not aggressive or irritating, like most security barriers.
- No personal data is collected or stored, complying with the European Union's General Data Protection Regulation.

Securing companies, protecting customers

The behavioural biometric data is compared to the historical behaviour of the user and average behaviour patterns. Based on analysed signals of each user profile, the system generates a 'trust score' with proprietary machine-learning algorithms. Assuming that the average person's phone habits will change, say, on a Saturday night compared to a Wednesday morning, the behavioural biometrics software then calculates whether someone is really who they are claiming to be.

arvato
BERTELSMANN

About Arvato Financial Solutions: Arvato Financial Solutions provides professional financial services centred on cash flow in all segments of the customer lifecycle: from identity, fraud, and credit risk management, to payment and financing services and debt collection. Our team made up of proven and reliable experts in around 20 countries gives businesses the best possible platform for growth.

www.finance.arvato.com

Click here for the company profile

As diverse protection methods are needed to cover a wide range of fraud cases, Arvato Financial Solutions offers a broad solution portfolio for different types of threats. Based on our long-standing industry and market-specific experience, the fraud and financial experts working in our teams offer a customised approach to each of our clients to provide the optimal solution for their particular needs.

Based on each company's individual goals, the industry landscape, the fraud prevention methods in place, and the fraud management architecture, we determine which specific solution or module combination is the best match for each business.

Arvato Financial Solutions is the backbone for growth, providing a holistic approach to help companies optimise their processes and customer experience, and protect their revenue and reputation while providing protection against fraud tailored to specific needs.

TrustStamp

Account Takeover and Step Up Authentication

About Andrew Gowasack: Andrew is Cofounder and Managing Director of Trust Stamp. As a co-leader in Emergent's global identity initiatives, Andrew is engaged with the delivery of identity-related services across all of Emergent's verticals, but his primary focus is building strategic partnerships around the World.

Andrew Gowasack | *Cofounder and Managing Director* | TrustStamp

True customer satisfaction means optimizing experiences and relationships from start to finish

In the digital age, businesses face the constant challenge of determining legitimate customers from fraudsters. Fraudsters target a variety of points along the transaction process, but some of the most common are new account creation, transactions, and account recovery. Enterprises must walk a fine line to ensure that appropriate measures are taken to prevent fraud while also providing a low-friction user experience. While the sophistication and frequency with which fraudsters attack has increased dramatically, so have the tools businesses can use to combat them.

One of the most prevalent forms of fraud is synthetic identity fraud, which results in direct losses of around **USD 118 billion each year**. This is a hard cost for many industries such as insurance, healthcare, and banking who typically rely upon flawed legacy authentication methods such as increasingly complex passwords, OTPs via text and email, and knowledge-based authentication (KBA).

However, as enterprises increase the complexity of the authentication process, legitimate users are confounded by that complexity leading to false positives and by users circumventing the intent of the systems (eg reusing passwords).

These legacy methods have been further compromised by the numerous high-profile breaches of retailers, healthcare providers, government records, credit bureaus, and hospitality chains, resulting in over 10 billion data records reported as being exposed since 2013 (Gartner Market Guide for Online Fraud Detection Published 31 January 2018 - ID G00318445), and those are just the ones that we know about!

With so much personal information readily available, fraudsters have become proficient at using the same data to commit multiple fraud attempts. Through the use of bots, fraudsters can submit tens of thousands of applications in a single day, typically from a remote country, and only need a handful to pass through in order to profit.

While the direct cost of **USD 118 billion** seems a staggering number, it is not the total cost. I had the opportunity to work directly with the fraud and risk team of a large US S&P 500 Bank who illustrated the extent of unseen opportunity costs. Thousands of potential customer applications were being rejected due to authentication concerns. While these applicants may have been fraudulent, they may also have been qualified customers. Moreover, the opportunity cost losses were not limited to new customers. →

A growing number of existing customers were locking themselves out of their accounts because they could not answer their KBA questions or they could not receive the OTP as they had changed their cell phone number. The standard protocol for the bank was to close these accounts.

These challenges are rampant on digital platforms. On average, for each account that is erroneously closed and each genuine applicant declined, there is an opportunity **cost of USD 61 per incident**. To make matters worse, there is an additional unquantified loss of goodwill. Just like the direct cost of fraud, these opportunity costs impact the companies' bottom line.

Because of their potential for security, as well as usability, a growing number of enterprises are implementing biometrics ranging from fingerprints to voice, to facial recognition. In addition to better technology for collecting biometrics (eg improving smartphone cameras), customers are becoming increasingly accustomed to using them. While biometrics' usability may resolve many authentication barriers, not all of them provide the technology needed to reduce the direct and opportunity costs of fraud.

Biometric solutions that can resist replay attacks and prove liveness partially resolve the issue of bot-initiated interactions. If a live biometric is required for applications, transaction approval, or account recovery, and that biometric is compared not just to the instant transaction but all prior biometrics from all transactions, then a fraudster needs a different live human for every transaction.

For many biometric solutions, a biometric sample is compared to a source of assumed truth such as a national ID document or passport, and if there is an apparent match, identity is established. The problem is that fraudsters create sophisticated fake IDs, sometimes using the same machines as legitimate issuing authorities, or they obtain "real" IDs for stolen identities. While this is not as scalable as blanked bot applications, it allows for repeated fraud attempts and has a far higher probability of success.

TrustStamp

About TrustStamp: A multi-factor biometric platform with inbuilt de-duplication that can be augmented with social media and other data mining and identity warranties. Among the platform's unique factor is a shareable non-PII hash that tokenizes identity and can embed both encrypted data and pivot points to external data.

www.truststamp.ai

Click here for the company profile

By using only biometric solutions that test liveness, while securely and compliantly storing biometric data, enterprises can compare the current biometric sample to all previous biometrics and spot instances where two or more users share the same biometrics. This deduplication process eliminates the possibility of the same person making multiple applications under different identities.

CA Technologies

Reconciling Consent in PSD2 and GDPR

Ecommerce continues to grow at an astounding rate – and so does online fraud. According to Javelin Research, card-not-present (CNP) fraud accounts for 81% of total fraud, representing billions of dollars in losses annually. To address this crisis, the industry is taking a fresh look at transaction authentication.

About James Rendell: James Rendell heads Payment Security Strategy and Product Management for CA Technologies. James is a recognised fraud and security expert, covering topics such as mobility, cryptography, ecommerce, and network and infrastructure security.

James Rendell | *Vice President, Payment Security Strategy* | CA Technologies

Why has authentication become such a hot topic?

First, let's compare Europe and North America because the landscape and the drivers are a bit different. In Europe, PSD2 is making it a legal requirement to apply authentication to any type of remote electronic interaction that carries a risk of fraud. In North America, the focus is more on optimising the customer experience by moving toward the frictionless checkout.

The card associations – Visa, Mastercard, and American Express – are also introducing global rules to make the use of these authentication programmes mandatory. Thus, ecommerce purchase authentication is critical in both geographies.

With the PSD2 regulation and new rules from the card associations, authentication has become the largest, brightest target on the ecommerce radar. And it's happening just as the 3-D Secure authentication protocol is launching. So the timing of EMV 3DS is spot-on.

Because we co-invented the 3-D Secure protocol, and we're one of the few providers that have been running the platform for 20 years, we can help get you there in the most efficient way. And I should add that we were the first to authenticate a EMV 3DS transaction.

How is artificial intelligence changing the authentication experience?

AI can evaluate any given transaction, using its unique contextual and transaction data. Whether it's a log-in event, a shopping transaction, or a new-product application, analytics can make a fine-grain decision about its implied or inherent risk. This is important for both driving out fraud and providing frictionless experiences.

> *"With the PSD2 regulation and new rules from the card associations, authentication has become the largest, brightest target on the ecommerce radar.*

For example, we've got hundreds of millions of identified devices associated with billions of ecommerce payments globally. We know if those past payments were high risk, confirmed as fraudulent, or confirmed as good. So we can say "We recognise this one; we've seen it before," and associate the device with known good or known bad behaviour. ➔

This intelligence, grounded in the ecommerce space, is a uniquely powerful consortium dataset to have. In the end, virtually every online crime, whether an account takeover, identity theft, or a malware compromise, ends up in a fraudulent payment attempt somewhere – often through the use of stolen user credentials such as online banking or card details.

On top of this, competing across multiple digital channels is very important to our customers. By providing a central, omnichannel platform for authentication of card and non-card ecommerce payments, we make it possible to manage these risks and customer experience demands.

What kinds of data do you need for risk analytics?

To be useful across geographies, analytics needs a really good consortium dataset. You need the largest possible pool of globally diverse risk and fraud data to draw on. But there's a common misconception that this data invades privacy, which is not the case. All the data we use for predictive modelling is anonymised to ensure that consumer privacy is protected. It is the patterns of use over time that are important, and the profiles that accumulate these patterns cannot be tied back to an individual.

Predictive analytics is actually a well-established fraud prevention discipline. It extended into the ecommerce 3-D Secure scene a decade ago, which is when the focus on gathering data to support its development became our core business. We have the longest established dataset in the ecommerce payment fraud field and we believe we have the largest market share of issuers in this space.

We service more than 13,000 card portfolios and well over a billion transactions a year. Having a globally diverse, large consortium of data for the analytics to chew on, as it were, is really important. Otherwise, you end up with predictive analytics that are trained out of very limited datasets, useful only for point problems.

How do you build an AI engine to fight fraud?

Certainly, the most important factor is that we employ a group of world-class data scientists with, when you add it all up, hundreds of years of experience in payment fraud.

ca technologies
A Broadcom Company

About CA Technologies: CA Technologies, a Broadcom company, is an industry leader in payment and identity fraud prevention, with friction-free transaction authentication powered by patented artificial intelligence. As a pioneer in analytics for online fraud, CA delivers a unique 360° view of transactions for issuers, processors, and merchants, across all payment schemes. Learn more at ca.com/balance.

www.ca.com

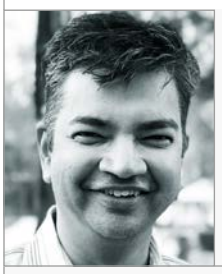
Click here for the company profile

You need this kind of expertise in knowing how to apply the techniques of data science. It's easy to make mistakes and misapply them, and there are plenty of war stories where a model was being biased the wrong way.

In the end, the more data you have, the more powerful the offerings you can build based on predictive analytics. It's about how you leverage data to build the advanced machine learning needed to optimise user experience and drive out fraud – while protecting consumer privacy at the same time.

Simility

Complex Fraud Threats Call for Adaptive Detection Tools



About Rahul Pangam : Rahul Pangam is the Co-Founder and CEO of Simility. He's an industry veteran, with impressive experience from Google, who is dedicated to empowering fraud fighters with the most adaptable, scalable, and accurate fraud analytics platform.

Rahul Pangam | *Co-Founder and CEO* | Simility

The payments and commerce landscape has undergone significant changes in recent years. At a local level, commerce and banking moved to a digital-first, standard format. At a global level, and specifically in developing markets, there has been a huge transition from "mum and dad" shops straight to online commerce. People no longer need banks or shops; they need banking and commerce services.

However, as much as this offers new and exciting online opportunities to businesses, unscrupulous individuals are also taking advantage of easy-to-access fraud tools and freshly breached data, exploiting vulnerabilities and targeting weaknesses in the security infrastructure of unsuspecting organisations.

Managing risk in a "post-breach world"

Companies are now operating in an environment in which they have to assume, even with the most sophisticated security solutions, that there are no cast-iron guarantees in a "post-breach normal" world. Managing risk in this environment needs to be handled in real time.

The most pressing challenge for companies is to balance customer experience effectively with security and regulatory issues. Customers have become accustomed to frictionless digital experiences and want payments to be made immediately. At the same time, cybercriminals are constantly evolving their attacks and using increasingly sophisticated techniques.

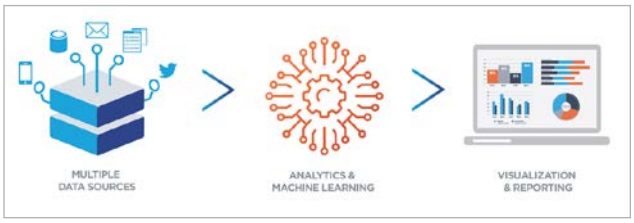
An increasingly complex regulatory environment that necessitates businesses to comply with PSD2 (Second Payment Services Directive), faster payments and open banking, adds a further burden to companies.

Fraud management is no longer a linear decision, with multiple factors needing to be considered and weighed in real time, which is something traditional tools are unable to accomplish. As cyberattacks become ever more complex, sophisticated, and cross-channel, companies need a solution that can change as business needs change, yet that can also protect against the evolving fraud landscape.

Balancing multiple priorities

Strong, but frictionless authentication is the key to offering an elegant customer experience and minimising fraud, while also staying in compliance. ➔

Although companies have attempted to improve security through different authentication methods, such as knowledge-based authentication (KBA) and multi-factor authentication (MFA), these methods are not without shortcomings. KBA lacks security because it is dependent upon “shared secrets” between users and servers, and MFA causes friction, which frustrates the customer. Businesses need a solution that empowers them to seamlessly balance multiple competing priorities without increasing friction, operational costs, or false positives.



Using data as a strategic advantage

As fraud continues to grow and cybercriminals become even more adept at circumventing security tools, it’s imperative to maintain a seamless experience for legitimate users. Using various types of data sources and applying concepts of machine learning for greater visualisation and accurate insights to drive effective fraud management is critical. Companies that can turn data into a strategic advantage will establish an edge over their competitors.

Built with a data-first approach in mind, Simility’s Adaptive Decisioning Platform offers a holistic view of the end customer. This helps companies orchestrate complex and accurate decisions to reduce friction, detect fraud patterns, and assist with regulatory requirements.

Simility’s complex authentication looks at various types of data, such as login, history, cross-channel interaction, behaviour, device, geolocation, etc to effectively and seamlessly decision the end user. Users are automatically accepted, rejected, or required to step-up, such as in the case of high-risk transactions. With Simility, companies do not only have the processing power to analyse huge datasets, but they can also customise user interactions. By personalising services based on risk factors, such as location, device and behaviour, trusted users can be identified and treated as such and provided with a more seamless experience, leading to increased customer satisfaction.

simility
A PayPal Service

About Simility: Simility offers real-time risk and fraud decisioning solutions to protect global businesses. Simility’s offerings are underpinned by the Adaptive Decisioning Platform built with a data-first approach to deliver continuous risk assurance. By combining artificial intelligence and big-data analytics, Simility helps businesses orchestrate complex decisions to reduce friction, improve trust, and solve complex fraud problems.

www.simility.com

Click here for the company profile

DataVisor

The Journey Towards Zero Factor Authentication

About Yinglian Xie: Yinglian is the CEO and Co-founder of DataVisor, a successful AI-based fraud detection technology company. Before founding DataVisor, Yinglian worked at Microsoft Research for more than seven years on numerous projects focused on advancing the security of online services with big data analytics and machine learning. Yinglian completed both her PhD and post-doctoral work in Computer Science at Carnegie Mellon University and holds over 20 patents.

Yinglian Xie | *CEO and co-founder* | DataVisor

From digital banking to online commerce, the consumption of online business services has changed consumer behaviour and expectations. Gone are the days when people were willing to stand in line to open a bank account or checkout at a retail store. Nowadays, they expect millisecond response at online marketplaces. They want to use emerging payment types like digital wallets. Peer-to-peer payments are on the rise. As a result, in today's digital economy, a well-orchestrated customer experience in digital channels is a competitive necessity, not a luxury.

The reality of creating an optimal customer experience, however, can be challenging. The cost of fraud for the financial services market has never been higher, owing largely to the proliferation of fraudulent online accounts. Competing objectives of revenue growth and risk mitigation mean that while businesses in this market are working to ensure that they can detect fraudulent accounts before they can wreak havoc, the added layers of authentication add friction to the customer user experience.

The **Q2 2018 Fraud Index Report** from my own company, DataVisor, showed a startling trend: as many as one in five cloud user accounts may be fake. In fact, for some cloud services, more than 75% of accounts may be used by hackers. More than 40% of application fraud comes from coordinated attacks, with single fraudsters operating multiple fraudulent accounts.

To combat this ever-growing rise in fraud, organisations are using multiple layers of authentication factors to verify the validity of a user's identity.

The emergence of n-factor authentication

Several types of authentication factors can typically come into play in preventing fraud, which are often combined for comprehensive protection. They include password factors (from ATM PINs to computer passwords), SMS factors (two-factor authentication codes), knowledge factors (username and passwords), possession factors (smart cards), and biometric factors (fingerprints or voice prints – or even optical scanning).

Proving online identity used to mean combining two or more of these factors, commonly referred to as "multi-factor authentication." This approach has been proven effective in enterprises of all sizes. In July 2018, Google reported that phishing attacks of its employees almost stopped after the company began requiring the use of two-factor authentication security keys across its business.

While multi-factor authentication increases the chances of detecting a fraudulent account or even possible identity theft, it is extremely cumbersome for users. In some cases, authentication happens to be based on data purchased from third parties, which consumers consider to be private information – like mortgage payments. Users typically balk at sharing so much personal information, and see it as an invasion of their privacy.

Moreover, multi-factor authentication does not even provide as much robust security as one might assume. Take, for example, the recent Facebook attack, where more than 30 million user accounts were hacked. →

Attackers manipulated access tokens to compromise normal user credentials. This is not surprising, especially when tokens are used to represent authenticated users and there is no re-authentication for subsequent interactions. The systems assume that these tokens are from real users.

The identity of the future

While technologists are busy inventing new methods to add another layer of authentication to identify users, at DataVisor, we are exploring the utopian vision of "zero factor authentication". This vision uses advanced technologies to build a digital DNA that integrates online behaviours (across device, activities, and biometrics) to uniquely identify each customer. With artificial intelligence, the reality of "zero factor authentication" is closer than we think.

There are three critical elements to realising the vision of zero factor authentication:

(1) Robust data collection: a more fine-grained data collection that forms the basis for deriving the digital DNA is imperative. Today, organisations suffer from data loss as it trickles into downstream systems. They lose their integrity and in that process lose valuable signals that could be used to build the digital identity. To be effective, organisations have to look into building and maintaining identities in real-time, using data streams at their source versus in batch.

(2) Constant analysis of data: this is an analysis in which users are continuously "re-authenticated," in passive mode, instead of using authentication at a given point in time.

(3) Transparency: when augmented with transparency and control, users become part of the customer journey, have better control and influence over how their identity is being built and used, and choose if they want to opt-in or opt out of zero factor authentication. Many companies like Google are allowing users to control the data they want to share and how that information gets used, thus users can choose their "own journey." The goals are to gradually establish confidence and trust in this new authentication paradigm, and to demonstrate that it is equally secure, or can, in fact, be more secure.

DATAVISOR

About DataVisor: DataVisor is the next-gen fraud detection platform based on cutting-edge AI technology. Using proprietary unsupervised machine learning algorithms, DataVisor helps restore trust in digital commerce by protecting businesses against financial and reputational damage caused by fake user accounts, account takeovers, and fraudulent transactions.

www.datavisor.com

Click here for the company profile

The next generation platform needs to rethink digital identity and authentication in a transformative way. Advances in technology must be able to combine machine and human intelligence to deliver zero factor authentication and not n-factor authentication. Current authentication methods expose too many loopholes – third-party apps, tokens, and APIs that can be leveraged by attackers.

Adding more layers of authentication simply means that as an industry we have failed to build a path to building a better digital identity. As AI becomes the driver for intellectual horsepower within the organisation, authentication means better security, greater trust, and personalised user journeys – all enabled by Zero-Authentication.

Aite Group

2019: The Push for Orchestrated Authentication

About Julie Conroy: Julie Conroy is research director at Aite Group focused on financial crime issues. She has extensive product management experience working with financial institutions, payments processors, and risk management companies, including several years leading the product team at Early Warning Services.

Julie Conroy | *Research Director* | Aite Group

Time is money when it comes to fighting fraud. Organised crime rings, fuelled with billions of compromised data records, are systematically and methodically targeting the financial services value chain with sophisticated card fraud, application fraud, and account takeover attacks. The volume of the attacks continues to increase, since there is little in the way of adverse consequences for the criminals (i.e., jail time).

Another key challenge for financial institution (FI) fraud executives is that even as the threat environment continues to escalate and rapidly evolve, FIs are under intense competitive pressure to make the banking experience easier and frictionless (while regulators in Europe appear to be taking the industry in a different direction, thanks to the second Payment Services Directive's requirement for Strong Customer Authentication). In the face of these seemingly contradictory mandates, many leading FIs are turning to orchestrated authentication.

What is orchestrated authentication?

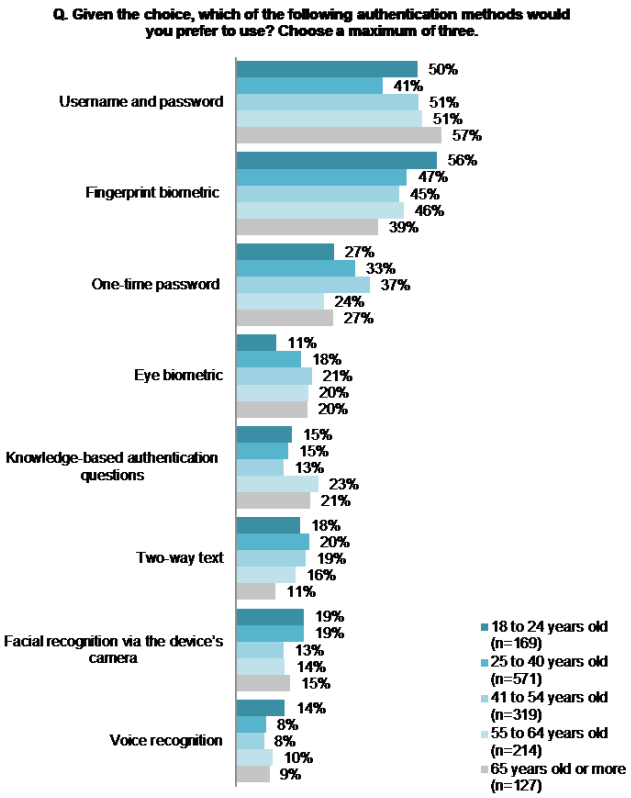
Nowadays, authentication is typically a one-size-fits-all activity, with stepped-up authenticators applied universally, regardless of the context of the transaction. For example, any time a retail-banking customer tries to send a person-to-person payment or a commercial customer tries to send a wire over a certain dollar amount, the user must input a one-time password. Orchestration of authentication seeks to better analyse the customer's usual behaviour patterns as well as the context of the transaction.

With orchestration, the friction of stepped-up authentication is only applied when necessary, that is when the analytics flag that the context of the transaction is unusual behaviour for the customer.

The concept of orchestration can also consider the end user's preferences in authenticators since this is by no means universal. The ability to tailor the authentication experience to the consumer's comfort zone is important since this increases the potential that the transaction will be completed, rather than abandoned. An Aite Group survey of consumers in the UK, US, and Singapore shows differing preferences for authentication mechanism by age, by country, and even by the frequency with which the consumer engages in digital commerce. A few examples of these differences can be seen in the figure below:

- Only 41% of consumers between 25 and 40 prefer username/password, compared with 57% of consumers 65 and older.
- 56% of consumers between ages 18 and 24 prefer the fingerprint biometric, compared with just 39% of consumers 65 and older. This is understandable since fingerprints wear over time and the fingerprint biometric is often difficult to use for seniors.
- Younger consumers are more open to facial recognition technologies than older generations. →

Figure 1: Consumers' Preferred Authentication Method by Age



Source: Aite Group survey of 1,400 consumers in the UK, the US, and Singapore, July 2018

Aite

About Aite Group: Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on financial services. With expertise in banking, insurance, wealth management, and capital markets, we partner with our clients, delivering insights to make their businesses smarter and stronger.

www.aitegroup.com

How is orchestration achieved?

While intuitive in concept, orchestration requires advanced analytical capabilities. To achieve the potential of orchestration, FIs need to be able to harness the breadth of their customer data and apply advanced analytics that can effectively understand customers' behaviour at the individual level, so that the decision of when to insert friction can be accurately taken. To enable consumer choice of authentication mechanism, the bank also must have a flexible range of authenticators available. To that end, many of the FIs on the forefront of this movement are approaching the process in a phased manner and either building or buying the requisite building blocks:

- **Data lake:** Many FIs on this journey are standing up their own bespoke data environment for orchestration (as well as other real-time fraud needs) or streaming the data directly into the risk engine, since data currency is important to effectively analyse the segment-of-one customer behaviour.
- **Advanced analytical engine:** Orchestration requires advanced, machine-learning based models that can baseline behaviour for individual customers, and then understand when their transactional activity deviates from the norm, thus requiring stepped-up authentication.
- **Authentication hub:** In order to provide a range of authentication options to customers, FIs are turning to platform-based authentication hubs that provide a range of authentication options, and make it easier for the FI to swap in new authenticators on an ongoing basis.

A handful of large FIs already have their initial iteration of orchestration in production, and 2019 will see more joining these ranks. Among those leading the way, there is a strong belief that the resulting enhancements to the customer journey will not only improve the bottom line, but will also prove to be a competitive differentiator over time.

FIDO Alliance

Open Banking: Why a New Approach to Authentication Is Key to its Success

About Brett McDowell: Brett McDowell helped establish the FIDO Alliance in 2012 to remove the world's dependency on passwords through open standards for strong authentication. Previously, he was head of ecosystem security at PayPal, where he developed strategies to improve online customer security.

Brett McDowell | *Executive Director* | FIDO Alliance

The concept of open banking promises users greater control over their financial data; however, it is not without risks, and its success is tied to consumer confidence when it comes to the security and privacy of their information. Indeed, ahead of the arrival of open banking in the UK, **a 2017 Accenture survey** of more than 2,000 British consumers found that two-thirds were not prepared to share their personal financial data with third-party providers. As Accenture's managing director Jeremy Light commented at the time, "Open banking has the potential to transform customers' relationship with financial products, but it hinges on consumers' willingness to embrace it."

Privacy concerns regarding the practice of "screen scraping" – where a third-party payment or financial data aggregation service accesses bank accounts on the consumer's behalf using their credentials – were surfaced by Barclays' managing director Catherine McGrath in response to the news of banking giant HSBC's foray into open banking with its aggregate app. The HSBC application pulled financial data from different bank accounts into one place for users. "With screen scraping, you have to give someone login details and then they can see absolutely everything; you don't have the ability to discriminate to say just six months' worth of transactional data," Ms McGrath said. "Our view is the best way for customers to share their data through APIs, so they are in charge of their data."

Regulatory implications and limitations

Around the world, regulations are emerging in line with the growing trend towards open banking. A prominent example is the second Payment Services Directive (PSD2), which came into effect in Europe at the start of 2018. PSD2 is being closely watched by other markets as open banking gains momentum, and regulated service providers navigate concerns regarding the implications for user privacy and security.

Whether or not these concerns ultimately slow Europe's adoption of open banking largely depends on how the Strong Customer Authentication requirements defined in the PSD2 Regulatory Technical Standard are enforced. To help ensure successful adoption of open banking, the FIDO Alliance has taken an active role in helping European regulators and API design groups understand how standards-based, modern authentication can be used to deprecate today's screen scraping practices while enabling a timely and secure migration to the open banking API model.

It is critical that open banking is implemented via modern APIs and protected by high assurance Strong Customer Authentication, as only an API-centred model is capable of protecting consumer privacy by providing granular access controls enabling the consumer to determine how much of their data is shared with any given third-party service provider. And only modern cryptographic-based authentication is fundamentally resistant to today's most common and effective account compromise attacks, such as phishing for passwords and even one-time-passcodes (OTP). →

Bolstering security, privacy, and usability with device-based authentication

New and improved methods of authentication are now available through open industry standards from the FIDO Alliance and **W3C**. Collectively known as FIDO Authentication, this innovative technology leverages on-device user verification such as the biometric capabilities on our mobile phones and combines this with interoperable protocols for strong cryptographic authentication. Biometrics is a compelling proposition for banks and other financial services companies, due to their ability to perform without dependency on the user remembering or sharing a password, greatly enhancing customer security while improving the user's authentication experience.

In practice, by utilising public key cryptography techniques in combination with "one touch" biometrics and/or security keys, the proliferation of smart devices can be used to provide stronger authentication without burdening users. If the customer uses their fingerprint, face, or PIN code to unlock their device, banks can now combine that same user verification method with strong cryptographic protocols made available through on-device platform APIs, including a Javascript API for web apps. This would allow customers to securely access their accounts online in full compliance with PSD2 strong customer authentication requirements, on both apps and websites.

Complying with SCA requirements – our approach

FIDO certification provides a clear path for financial services organisations to comply with PSD2 strong customer authentication requirements.

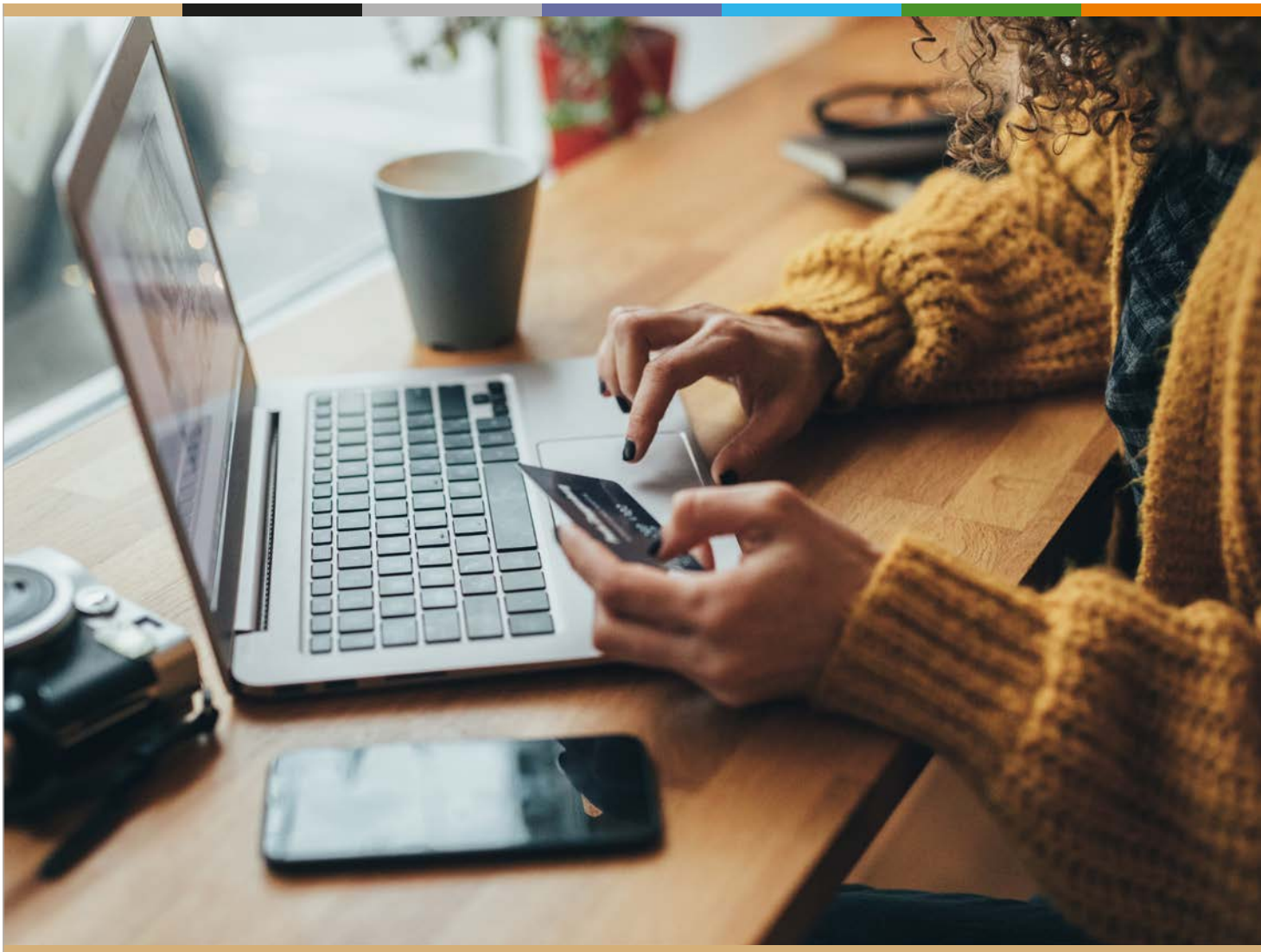
The FIDO Alliance's authentication standards provide a scalable way for the European financial ecosystem to meet PSD2 requirements for strong authentication of user logins and cryptographically signed transactions, while also meeting organisational and consumer demand for transaction convenience. FIDO certification programmes offer an independent validation of implementations conformance, interoperability, security, and even biometric performance when applicable. All certified devices are eligible to be listed in a public registry of device metadata that enables a financial service to evaluate the security properties of the device, ensuring the device's ability to comply with the restricted operating environment requirements detailed in the PSD2 RTS.

About FIDO Alliance: The FIDO Alliance works to address the lack of interoperability among strong authentication technologies and to remedy the problems users face managing multiple passwords. The Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms which reduce reliance on passwords.

www.fidoalliance.org

PSD2 should significantly improve the way third-parties access account data. Ultimately, public trust is essential for momentum to continue to build around open banking and to ensure its enduring success. In order to build and maintain this confidence, a new approach to authentication must be taken in which there are adopted far superior modern methods that will enhance security and usability to the benefit of all concerned.

Customer Onboarding and Digital Identity Verification



Customer Onboarding and Identity Verification

An Introduction to Customer Onboarding and Digital Identity Verification

Mirela Ciobanu | *Senior Editor* | The Paypers

Did you know that 59**% of customers looking to open a bank account have walked away from online applications in the last 12 months**? The reason behind this: many application processes aren't really designed for the digital age.

However, the good news is that **smart fintech businesses** and **challenger banks** are getting under the skin of digital identity and using our uniqueness to unlock a frictionless future. They do so **by tapping into technology** such as **behavioural biometrics, machine learning** and **artificial intelligence**, and lately also blockchain to support secure, intuitive and personalised digital experiences that are beneficial for both companies and consumers alike.

In this chapter, we will see **how the onboarding process looks like**, not only from a **customer's perspective** working with a financial services institution (FI) or other regulated entities, but also from a **FI's perspective onboarding new clients**. Banks are looking for ways to increase conversion of new customers applying for their product/service, be relevant for them, while also **managing risks associated with KYC**/onboarding processes. But customers are demanding **a flexible (mobile first) and modular onboarding process**, and regulators are constantly watching the market and updated/adopt new regulations (e.g. AMLD5).

Will banks be able to get this puzzle right, in time? After all, improving the customer onboarding experience should be a priority for financial institutions, especially since regulations such as PSD2 will enable customers to change their financial service provider more easily.

Onboarding new customers in a digital world: a bank's perspective

After a few years of battles between incumbent banks and smart fintechs/challengers, everyone has agreed that **digital customers need digital processes**. Nowadays, for many financial services organisations, the onboarding process is considered costly, prone to fraud and creates unnecessary friction in the customer's experience. This old approach is simply not sustainable as it gives rise to high abandon rates and does not meet the expectations of a younger digitally 'native' customer.

How is my current onboarding process performing? The incumbents

Because many application processes aren't really designed for the digital age, incumbent banks just replicate traditional onboarding processes, pushing only some parts of it online. As a result, **up to half of digital applicants can't actually complete an application online**; instead, they have to go into a branch to verify their identities, or submit additional documentation. →

An Introduction to Customer Onboarding and Digital Identity Verification

In 2016, Signicat conducted a research called the Battle to On-board that aimed to portray the onboarding processes for the UK financial services consumers. The research found that **40% of consumers had abandoned bank applications**; more than 1 in 3 (39%) abandonments were due to the length of time taken and a third (34%) were due to **demanding too much personal information**. Interestingly, the company performed the same research two years later and the results **were similarly devastating for banks**. In fact, it was worse than ever in the UK, with 56% of respondents having abandoned an application. Among other impediments for applying cited by consumers were the fact that they **had to provide personal information by post or take it into the branch**, and sometimes **the language used by the bank was confusing**.

Nevertheless, some progress has been made with banks such as China Merchant Bank, one of the largest credit card companies in China, Wells Fargo and the Bank of America that have **reached out to AI assistants to improve customer experience**. For instance, **Bank of America's 'Erica' chatbot** was designed to maximise the opportunities of the growing demand for mobile banking and is capable of anticipating the financial needs of each individual customer and sending them personal smart recommendations to help them achieve their financial goals.

In Europe, most innovative banks such as **ABN AMRO, CaixaBank** and **BBVA** have developed their own hassle-free banking brands to cater for millennials and digital savvy users. For instance, in Spain, CaixaBank **launched in 2016** ***imaginBank***, a mobile banking service that enables users to control their finances, view their account securely within Facebook, or draw money from an ATM without a card and send money to friends using only a mobile number. Similarly, present in the Netherlands, Germany, Belgium and Austria, Moneyou, a brand of ABN AMRO, is a mobile banking service connected to a mobile app called Tikkie. The app can be used by anyone, regardless of who they bank with; it is only necessary that the person receiving the money to have the app. Once the users enter their name, mobile phone number and the IBAN number, they can start sending payment requests via WhatsApp, Facebook Messenger, Telegram, QR-code or text (SMS).

How is my current onboarding process performing – the challengers

Even from the first encounter with the clients, challengers have been praised for providing great user experience. And why is that? They **are digital**, they can develop from scratch, **have smaller product offering**, they do **not depend on legacy systems**, and are **adopting new technologies** to automate identity verification processes.

For example, **Fidor Bank, a German online bank, founded in 2009**, has a simplified, three-stage process of onboarding depending on two essential variables: customer behaviour and product complexity. For the Fidor's Smart Cash Account product, the entry point for a new customer is to join the Fidor community, by supplying one's credentials from Facebook, with no obligation to buy anything. Step two is obtaining a pre-funded online 'wallet' that can be used to move money within a closed loop as the user graduates to being a 'customer' after passing reduced KYC. This allows him or her to test out Fidor, again without any further commitment, while still being part of the community. The third and last step is to open a more traditional account after passing full KYC. Now the customer can also trade commodities, FX, and digital currencies. ➔

An Introduction to Customer Onboarding and Digital Identity Verification

So, the Fidor Smart Cash Account **behaves according to the way the customer registers**, not according to a bank-imposed process.

In general, banks must check the identity of everyone opening an account to prevent money laundering or other criminal financing activities. While these ID checks used to take place exclusively at bank counters, nowadays many services use video identification - customers rotate their ID card in front of a camera allowing staff to check for security features, like holograms - or just selfies.

However, **this simplicity might come at a cost**. **Germany's N26 could be potentially vulnerable to money laundering** and terrorism financing, according to a German publication WirtschaftsWoche, which exposed a security gap at the online banking startup. As the fintech rolled out a selfie validation procedure for account opening, it is easier for criminals to open accounts with fake IDs. A WirtschaftsWoche correspondent saw how a man scanned a friend's ID, added his own passport photo to the ID, printed it out and stuck it atop of a white plastic card that was the same size as the office ID card in his country. He cut the edges to make them round and the result was a new identification card that could be used to open a new bank account.

"Go online or go home" – ways to improve it

INNOPAY developed a Benchmark that provides banks with **essential insights into how to make a good first impression on customers**. INNOPAY consultants have identified six key actions that banks should execute in order to provide the prospective customers the best-possible onboarding experience and increase conversion rates.

1. Eliminate all **channel breaks** to support an end-to-end fully digital onboarding experience. For example, banks should adopt paperless onboarding processes as well as processes for which no physical signature is required.
2. Make required onboarding information and prerequisites **transparent** and understandable for the user. For instance, clear information and communication are key, so that the potential customer has all relevant details at hand and can run through the process in a smooth way.
3. Guide the customer through the onboarding flow and empower **customer support** to help prospects during onboarding in a quick and high-quality manner. The end result is that the prospects always know where they are currently positioned within the process and find information quickly. If they do not understand why the bank is asking for certain information or why the bank requires the prospect to use a certain identification method, they can rely on professional support provided by the bank.
4. Make use of **tools** that ease the process of data entry and eliminate errors. Thus, errors can be prevented by various in-process validation tools to increase conversion and also to reduce manual efforts by the bank, leading to cost reduction.
5. Enable customers to **instantly login** and start using the payment account after a successful onboarding.
6. Deliver a **consistent look and feel** throughout the whole onboarding experience. →

An Introduction to Customer Onboarding and Digital Identity Verification

Overall, we can conclude that banks can stay relevant for their customers if they transform the entire on-boarding process online. So far, we have seen that consumers are more likely to apply for a product if the process is 100% online and if paper-based identity checks are eliminated.

Moreover, the onboarding process could be accelerated if they could use their verified physical ID, such as a passport or driving license, and here, in the 100%-online application process, an important role is played by identity verification.

Identity verification: some last thoughts

Identity verification is proving that specific identity attributes are actually connected to the person, entity, or thing that they are intended to represent. **According to Josje Fiolet**, Digital Onboarding lead at INNOPAY, video identification, reading the chip of the document via NFC (Near-Field Communication), using eID solutions, or taking a picture of the ID document can enable businesses to answer questions such as 'Is the customer's document valid?', or 'Is the person really who he/she claims to be?'.

To build a reliable profile of the customer, other techniques can also be considered. The trail of data that we leave behind may not be an identification method in itself, but it can serve as an additional step when building a trustworthy profile. For example, our activity on social networks can be used to provide a certain level of assurance of someone's identity, and the account's profile picture can be matched with the picture in the identification document.

For effective client identification, a business must have access to a range of technology solutions that can indicate the veracity of an individual along with providing access to worldwide trusted datasets that contain billions of data elements of information from governments/public bodies, including global postal, telecoms and other public data, to validate the underlying data associated with financial services provision. Not only does this deliver a 360-degree view of the individual, but it also authenticates who they are.

The key to all these lies in balancing these elements in order to create perfectly tailored products. By understanding the unique needs of customers, financial businesses can help governments and major institutions fight fraud and grant access to underserved and legitimate customers. We can conclude by underlying one of Money 2020's ideas from the 2018 edition: once we solve this puzzle of identity custodianship, we can craft a masterpiece in which uniqueness is celebrated, protected and used responsibly.

Melissa Global Intelligence

The Paypers sat down with Barley Laing, the Managing Director of Melissa Global Intelligence, to discuss the latest ID verification and KYC trends and developments in the financial industry.

About Barley Laing: Barley Laing is Managing Director at Melissa Global Intelligence, where he leads commercial and operational activities, helping the organisation to become a global leader in identity and data verification services. Previously, Barley was CEO of World Address and 2L Technologies, and has held senior positions at Xerox, British Telecom, ADC and Shell.

Barley Laing | *Managing Director* | Melissa Global Intelligence

How would you describe Melissa for those who are not familiar with the company?

Melissa is a leading provider of global identity verification solutions, utilising innovative technology to provide our clients with a data-driven competitive advantage and enhanced Know Your Customer (KYC) and Anti-Money Laundering (AML) processes to help combat fraud.

How can financial institutions that are looking to comply with AML take advantage of Melissa's services to deliver on the customer's expectation for convenience, speed and simplicity, while also mitigating the risk of fraud?

21st century customers expect quick and secure financial service provision – if the consumer experience is poor, they will move to another provider who can deliver a better outcome. Melissa offers a range of global identity verification solutions that are easily integrated into existing customer service platforms and IT systems. Melissa's solutions range from 'proof of address' check to full biometrics that authenticate customers in real-time. Using Melissa enables organisations to retire costly legacy systems, reduce headcount for manual review, and avoid reputational risk. Regulatory AML checks are completed in a fraction of a second, where manual review could take days to complete. By using Melissa, access to global identity data, sanctions and watchlists are one click away – speeding the processing of applications. AML Screening is an important step in determining the risk of an individual, to make sure business is not being conducted with those committing money laundering or financing terrorism. Melissa screens against global sanctions and PEP checks (Politically Exposed Person), a database containing information on world leaders for 200+ countries.

> *"21st century customers expect quick and secure financial service provision. Melissa's wide range of global identity solutions authenticate customers in real-time so organisations don't have to compromise the customer's experience while mitigating the risk of fraud.*

A cornerstone of global anti-money laundering controls are the KYC processes/requirements. How does Melissa perform such processes?

Melissa can quickly perform KYC through our ID Verification solutions (IDV), providing access to global datasets containing billions of trusted identity elements from the government, global postal, telecoms data and other data sources in real-time. The underlying data provided at input can be cross-checked, building a confidence score for the applicant based on strength of the underlying data. Melissa helps further by identifying individuals at the 'point of entry' via imaging and facial recognition technology. →

This is done by checking the applicant by cross-referencing a live image (biometric facial recognition of a selfie) against a scanned ID document image (eg driver license photo). ID documents are validated to ensure they are not fake, and the held data uplifted via Optical Character Recognition (OCR) to avoid mistakes being made at application.

How would you explain the difference between effective client identification and poor KYC standards?

This difference can be categorised depending on perspective:

Consumers want a slick application process. If the supplier organisation can quickly establish a customer's ID, the consumer will have confidence in that provider.

Financial Service Organisations with poor KYC processes can lose customers at application, but this could also lead to fraud and compliance issues that will impact their brand and bottom line. Using modern KYC initiatives effectively can mean better sales and increased customer engagement.

Fraudsters actively target organisations with poor KYC processes, they know less effective ID resolution means easier victims.

Your product package includes a solution that addresses ID verification that gathers data in order to complete People Data. As sometimes not all gathered data is useful, how does your solution maximise the value of this data?

Research shows many ID checks fail from incorrect data entry, organisations can waste money by running ID checks that are destined to fail because the basic data veracity was not confirmed first. Melissa's solution ensures underlying data is correct before performing the ID check, this happens in fractions of a second and without disruption to the customer. Having a complete and validated identity record of a customer means that organisations will better communicate, and can complete transactions with their client base in confidence, maximising the value of their customer data.

Can you identify possible trends in ID verification? And what can we expect in the next five years?

In the next five years I expect that:

- As artificial intelligence helps brands engage with consumers more efficiently, it could evolve to play a role in ID verification in a way that helps brands to deliver a seamless customer experience.
- The role of behavioural biometrics in ID verification will grow and evolve. This could include monitoring how people type on the keyboard and use the mouse or touchscreen. It could become an important way to authenticate an ID.
- Augmented intelligence will play a key role along with artificial intelligence, working to enhance human intelligence. For identity verification, it will mean not only smarter intelligence, but also stronger intelligence.

In the shorter term:

- Growth in facial recognition technology will confirm ID.
- As consumers increasingly worry about their ID being stolen, there will be a strong evolution in technology that verifies and protects customer data, as brands seek to placate their fears.
- Fraud is a growing global issue, we see IDV becoming the norm across all sectors and service provision beyond financial services.

Trulioo

Hard Problems: Identity Verification, Fraud Prevention and the Giant Leap Towards Financial Inclusion

About Zac Cohen: Zac Cohen is a versatile leader experienced in managing and scaling high-growth companies. Zac is currently the General Manager at Trulioo – a hyper-growth Vancouver startup solving global identity challenges associated with international regulatory compliance, fraud prevention, and trust and safety online. He is passionate about fostering change-makers who want to make an impact and are engaged in building groundbreaking solutions to solve our world's most pressing problems.

Zac Cohen | *General Manager* | Trulioo

At the turn of this decade, the "GDP of the internet" began rising precipitously; online merchants, particularly micro-merchants, began opening online storefronts in increasing numbers. Yet the technology powering the flow of money online was simply not keeping pace. It was this set of unique circumstances that necessitated the creation of a new generation of payment solutions. With their elegantly simple code and their vast network of relationships with credit card issuers, banks and financial services, these payment solutions open the doors to a truly borderless marketplace where online merchants and buyers could transact freely.

A layer of trust

There was, however, another problem that stood in the way: If these payment solutions wanted to enter new markets, particularly unchartered and unfamiliar ones, they needed to first build a layer of trust between themselves and their new customers – the online merchants.

This layer of trust needs to be built on:

- Customer due diligence (CDD): Ensuring a level of CDD that is commensurate with the risks involved in transacting with new customers in these regions. For payment companies, banks, and financial services providers, this includes meeting regulatory requirements such as **Know Your Customer (KYC)**, **Anti-Money Laundering (AML)**.
- Fraud prevention: While the digital economy has created unprecedented opportunities for both established and upstart merchants around the world, it is also prone to fraud. Indeed, prevention is the operative word here, because very often fraud is only detected after the fact.

The challenge

As it happens, the success of both CDD and fraud prevention hinge on a critical process: Identity verification. When it comes to highly competitive and fast-growing companies, it becomes imperative to move quickly and capture as much market share as possible. For these companies, it becomes essential to have an identity verification process that can scale quickly, efficiently, and cost-effectively. In order to do that, these companies need access to a variety of trusted and reliable data sources; but, as it happens, the data that is being sought to verify the identity of merchants in these markets is often available exclusively with local data vendors.

Consider a growing payments company; let's say it is foraying into the Peruvian market. It will likely struggle to forge relationships with local data partners there; it would have to sign multiple contracts with multiple data partners in order to gain access to a sufficiently large swathe of identity data. This process requires a great deal of time, resources and familiarity with the local ecosystem; identifying, procuring, and vetting data sources, and then manually undertaking security and compliance checks. Even from a technology standpoint, the time and investment required to build an API for every data source that the company intends to tap into, become critical roadblocks to their expansion plans. Given these constraints, it would take anywhere between six months to a year for these companies to integrate each data source onto their systems. Now, consider the total time it would take to integrate with multiple data sources across multiple countries; that's when the project begins to look unfeasible. →

The solution: a single API to access identity data across the world

Trulioo has, to a large extent, mitigated this problem; as one of the world's preeminent identity verification solutions, we have access to hundreds of data sources. Through a single API, **GlobalGateway** -- Trulioo's flagship solution -- provides secure access to over 400 data sources across the world. With GlobalGateway, our clients no longer need to sign multiple contracts with multiple parties; instead, a single contract with Trulioo provisions it with access to data from multiple data partners. In fact, one of the world's leading cross-border payroll solutions uses GlobalGateway to verify the identity of payees in 52 countries across different continents, including Chile, Jordan and Egypt.

Instant access to a plethora of data sources also goes a long way in mitigating risk; for instance, companies tend to put off their CDD process till such time as a merchant starts transacting beyond a certain dollar threshold — this is mainly because traditional processes of identity verification were manual, slow and required much human effort. The instantaneity of identity verification, which Trulioo enables, allows companies to place identity verification at the very beginning of **merchant onboarding**; the same instantaneity makes it easy for many of our clients to verify (rather, reverify) the identities of their existing merchants. As a result, our clients are able to understand their entire consumer base quickly and take timely cognizance of any risks that their merchants might pose.

Mobile ID verification: a boost for financial inclusion and an antidote to fraud prevention

From very early on, we, at Trulioo, saw identity verification as a catalyst for financial inclusion; to that end, we realised that we needed to cover hard-to-reach areas, which lacked traditional sources of identity data. As of October, Trulioo can verify the identity of up to **five billion people**, or two-thirds of the world's population, along with 250 million businesses, including micro-merchants. In developing areas of the world, where a large part of the population is "unbanked", and traditional sources of identity data have limited coverage, **mobile network operators** (MNOs) can play a game-changing role. In developing markets, the mobile user base outstrips that of financial services: for instance, over the last four years, over a billion mobile accounts were opened around the world, compared to 500 million bank accounts. Indeed, the data in possession of MNOs can go a long way in verifying the identity of otherwise "thin-file" merchants.

Trulioo
Building Trust Online

About Trulioo: Trulioo is a global identity verification company providing advanced analytics from traditional and alternative data sources to verify identities in real-time. Through GlobalGateway, Trulioo's electronic verification platform, clients are able to streamline their cross-border compliance needs, helping them meet Anti-Money Laundering and Know Your Customer requirements, while simultaneously mitigating fraud and reducing risk.

www.trulioo.com

Click here for the company profile

To that end, **we began partnering** with MNOs around the world. Currently, we have access to identity data provided by dozens of MNOs, which cover 1.8 billion mobile users. When the traditional KYC-compliant sources of data are combined with MNO data, one is able to obtain more insight into the identity that one is trying to verify. No less important is the added value that MNOs bring to fraud prevention; for example, when verifying a merchant's mobile number against MNO data, GlobalGateway can flag numbers that are VoIP numbers, which are often prone to misuse by fraudsters.

We are one breakthrough away from financial inclusion

If we look back at the evolution of online commerce, we realise that at different points, there have been different technological breakthroughs that have catalysed the sector in different ways. The revolution in online payments was one such breakthrough; identity verification is on the cusp of being the next breakthrough. Today, merchants from around the world can transact online as free agents of the online economy; our dream is to see a world where they are able to transact not just as free agents but equals of a financially inclusive ecosystem.

INNOPAY

Digitising Complex Onboarding Processes: Who Will Be Leading in Getting It Right?

About Josje Fiolet: At INNOPAY Josje leads the Digital Onboarding practice. She has a background in digital banking, digital identity, and fintech. Her speciality is combining regulatory requirements, customer preferences, and organisational capabilities.

About Guy Rutten: Consultant, Digital Onboarding Specialist, Guy is an experienced product owner and analyst working on onboarding processes for digital banking applications.

Josje Fiolet | *Manager, Lead Digital Onboarding* | INNOPAY Guy Rutten | *Consultant* | INNOPAY

In the past year, customer onboarding processes for simple financial products have become much more convenient. The **INNOPAY Onboarding Benchmark (2018)** shows that almost all Dutch banks now have a customer friendly, digital onboarding process for opening a payment account, inspired by the challengers like Revolut, N26, and Monzo offer across Europe. Thinking about how much the market has changed in the past year, it is only a matter of time before onboarding of more complex products will be digitised as well. So the question is: who will be leading in getting it right, banks or fintech?

For more complex products the onboarding process is still very complex and cumbersome, as non-digital steps are involved. Complex products have stricter regulatory and risk requirements – and with AMLD4 set into national law in 2018 and AMLD5 already coming up, no leniency is expected any time soon. Regulation is often seen as an impediment to customer facing innovation and perceived as a trade-off for user experience. At INNOPAY we see this differently. Existing technologies can both enhance the customer experience and improve the security of the onboarding process.

For banks, it is time to approach onboarding from this perspective. First, because consumers expect a fast and fully digital experience. In a commoditised business like transactions this is becoming the differentiating experience. Second, because compliance cost for both implementation and accuracy will rise if manual operations are maintained. People checking documents and re-entering data are both expensive as well as error prone. It is expected that digital challengers will change the onboarding landscape for complex products in the same way they did for the “simple” products. However, established players still manage to keep challengers at length, as they have the advantage of a large and typically loyal customer. But for how long? Let’s talk about what is needed to keep it that way.

1. From risk at the product level, to risk at the customer level

Obviously, not all customers are the same and therefore the risk profile differs per customer. Banks, however, are used to determine the risk involved at product level measuring every customer against the same stick. The onboarding process for complex products has become unnecessarily difficult for most customers, having a negative impact on the user experience and conversion ratios. Furthermore, the process forces banks to put the same effort in the low as well as the higher customer risk profiles in terms of data gathering, file creation and monitoring. A personalised process can save time and cost for both the customer and the bank.

2. Modular onboarding building blocks

Onboarding processes preferably cater for a variety of contexts, as explained above. Modular building blocks form the basis for processes that serve different products, customers and channels. ➔

The onboarding process can be designed with different sets of building blocks, which might vary given the specific relevant context. The required level of compliance and the risk involved can be used to determine which building blocks apply for a specific situation.

Within the different building blocks, new technologies can and should be used to add both security and convenience for the customer and bank. Innovative technologies are often perceived as risky due to lack of experience and best practices. Fortunately, the European Supervisory Authorities (ESAs) are helping out. They published a **guideline** with questions that help banks assess if an innovative solution is fit for purpose. In short, ESA's guidance determines not if, but how new technology can be used to optimise a building block.

3. Start small with the end in mind

So, how to design and implement a more personalised and modular process, using technology in a controlled manner, as described by the ESAs? Improving the onboarding process is quite complex as it touches upon so many systems and departments. A good start is to describe the ideal process. After setting the end goal, the process should be split up in building blocks that can be optimised separately. This enables banks to focus on operational effort per building block, rather than having to change everything at once.

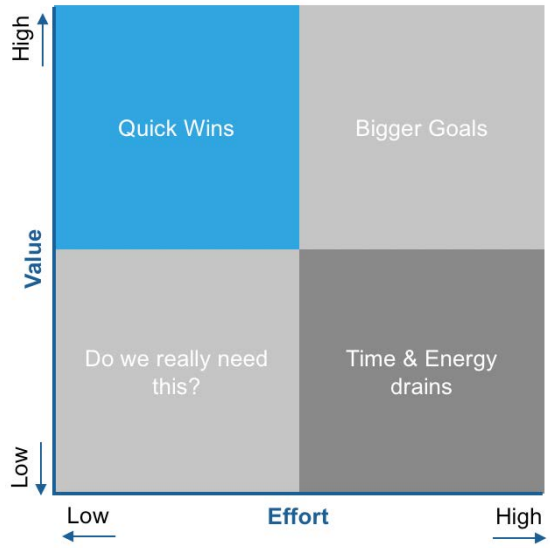


Figure 1: Effort x Value matrix to prioritise activities

INNOPAY

About INNOPAY: INNOPAY has a strong international track record as innovation expert in the digital transactions space. Our aim is to help companies, organisations, and consortia develop innovation strategies, co-create new products and services, and digitally transform their business models.

www.innopay.com

To prioritise initiatives, the simple yet effective "Effort x Value matrix" can be used. The focus should be on the Quick Wins. "Quick Wins" are improvements that require relatively little implementation effort and have a big impact on the value created. Examples are improvements in user experience like automated document read and reduced number of required data fields. Not only will the customer experience improve as straight-through processing ratios will increase, but also data quality will improve, enabling banks to enhance decision making on how to best monitor customers going forward.

The Quick Wins can only be derived from picturing the "Bigger Goals". Working incrementally will lead to quicker results, a steeper learning curve, easier buy-in of internal stakeholders, and most importantly, it shows the customer you are taking them seriously by continuously improving the journey.

To conclude, a step by step approach, using new available technologies in a modular way, can help financial institutions to digitise more complex products, make processes more secure, and most important, keep their customers satisfied and loyal in return. So maybe this time the banks will lead the way!

Steve Cook

Intro Steve Cook on latest trends in biometrics technology and the value of biometric authentication for the KYC process

About Steve Cook: Steve Cook is an independent biometrics and fintech consultant, helping banks, ecommerce enterprises and fintech startups to navigate the complex world of biometrics. He advises financial institutions regarding their deployment of biometric authentication and digital identity strategies; assisting in the process of vendor selection, biometric modalities and types of solutions. Steve has over six years' experience in the biometrics industry previously with Daon and Facebanx. He now operates his own consultancy business **Biometrics for eCommerce** and he is currently providing services to a fintech startup FaceTec as well as a major European bank.

Steve Cook | *Biometrics and Fintech Consultant*

What's new on the biometrics technology market and which method seems to have a greater potential?

Behavioural biometrics is one of the fastest growing of all the biometric sciences and there are many new fintech companies offering different types of solutions. Sometimes known as passive biometrics, it usually involves the customer not doing anything unusual during a user session.

Behavioural biometrics also provides an analytical tool to moderate risk. It actually monitors the user's behaviour during the visit and detects anomalous activity. There are some 2,000 parameters that behavioural biometrics depends on and they give a clear indication of someone's unique identity. These range from monitoring human motion gestures and patterns to keystroke dynamics and factors – such as speed, flow, touch, sensitive pressure, and even signature formats. They also use machine learning and AI as a continuous form of authentication.

Combining a number of biometrics in a step-up process or what is called multimodal biometrics would be used in cases where higher risk transactions are processed. This happens in order to prove someone's identity, known as Strong Customer Authentication.

Some organisations prefer biometric authentication to be stored on the device, or as a server-based solution known as on premise, or as a SaaS cloud deployment known as software as a service model. The SaaS model is currently proving to be the most popular.

How does biometrics augment the KYC process in order to assure compliance?

Biometric technology forms one part of the KYC process and it can be used in the remote on-boarding channel when signing up new customers. Typically, the biometric data, such as your face, is captured together with an ID document, like a passport or driving license, via a smartphone's camera. The ID document data can be verified separately through known third parties. The face data is compared with a live face capture and the photo ID for a comparison match. Then a risk score can be applied to the matching process.

> *"Banking and ecommerce are just some of the channels that we are seeing where biometrics are becoming standard in the areas of digital identity and KYC.*

It is important to state that it's nearly impossible to prove that an ID document is 100% genuine through existing digital methods. NFC can read the biometric chip on a passport to obtain the original data and this can be verified. →

However, some sophisticated fraudulent passports can still fool the system. Using the liveness functionality during the on-boarding session helps to prove the person is there in real time, but proving the true identity has to rely on other checks. Most Government databases are not accessible for commercial use in order to verify people, thus remote digital on-boarding does carry some risks.

What benefits does biometrics for KYC management bring for banks?

For branch banking, biometrics can be captured within a store via a tablet and, generally, bank staff will use the device for on-boarding new customers with proof of ID. However, we are seeing this trend shifting away from traditional branch banking towards online and mobile.

Digital on-boarding is proving to be extremely popular with the tech savvy generation known as the millennials. This generation is doing most things via their smartphone; whether it is retail purchases, social media, or gaming. Mobile digital banking is becoming more popular amongst **the 18-35 year olds and by the end of 2018 it will overtake online**, telephone, and branch banking combined.

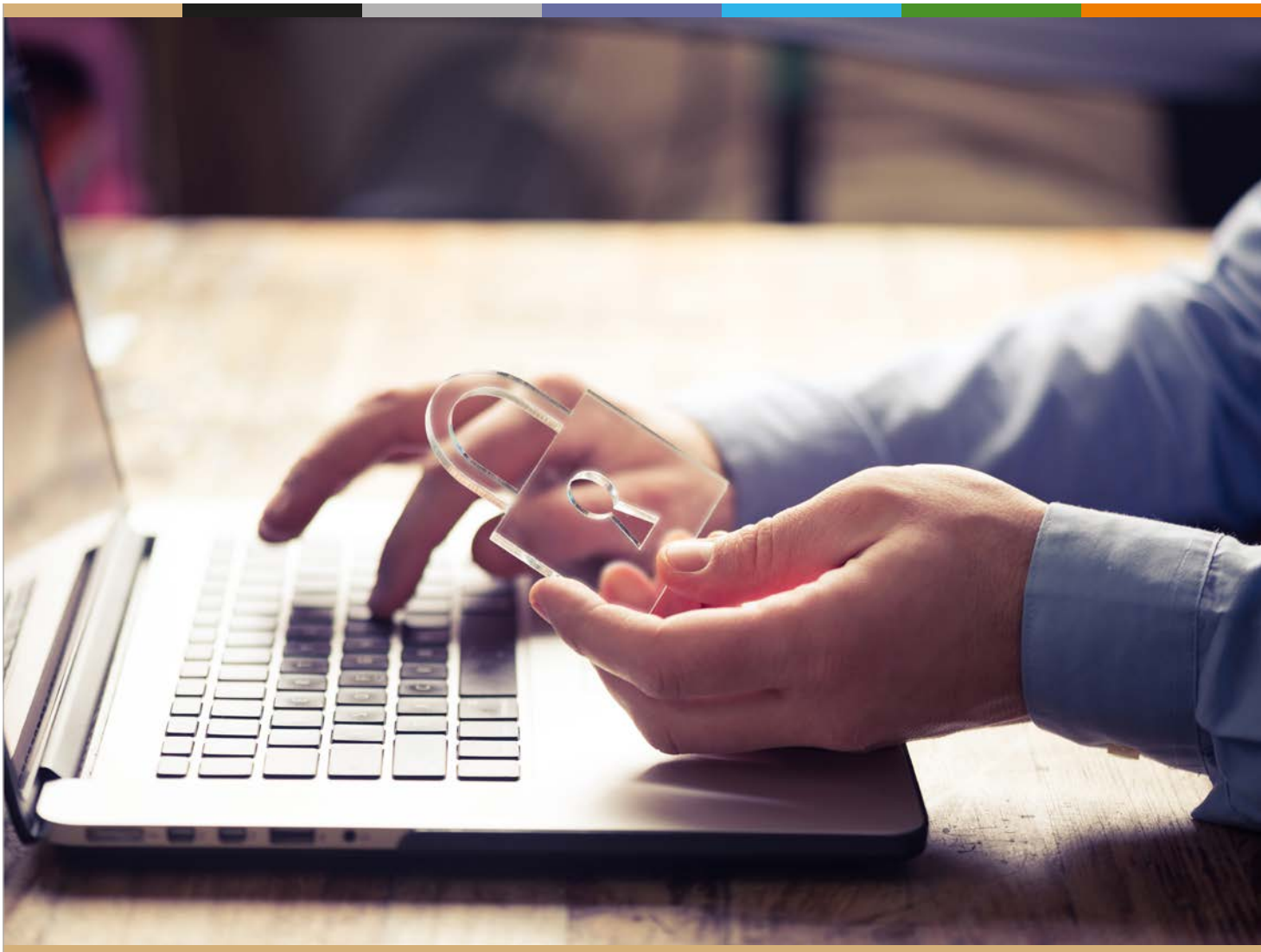
In 2010, **branch banking accounted for around 70% of all banking**. By 2020, it could be as low as 15-20%, while digital banking will reach a staggering 80%. Today, bank branches are closing at a rate of around 60 per week in the UK alone. All the large banks have to adapt quickly to the new customer trends for more digital-only platforms. Many new challenger banks have launched innovative banking services via digital channels and are in direct competition with the more established branch banks.

Do you think biometric authentication will become a norm one day or a standard for automation of KYC procedures in sectors such as banking and ecommerce?

Biometric technology is already becoming the norm in many verticals: from aviation and automation to education, health, insurance, and retail. Banking and ecommerce are just some of the channels that we are seeing where biometrics is becoming a standard in digital identity and KYC areas.

According to **Goode Intelligence**, by 2020, 1.9 billion bank customers will adopt biometrics for a variety of financial services, including ATM cash withdrawals, proving identity for digital on-boarding, accessing digital bank services through IoT devices and mobile bank app authentication. Biometric authentication for banking purposes is going to generate USD 4.8 billion in revenue by 2023. I believe biometric authentication will become ubiquitous everywhere and we will be able to eventually say goodbye to the “passwords”.


KNOW
2019
LAS VEGAS
MARCH 24-27, 2019
ARIA • LAS VEGAS
Where We Define
the Future of Trust
Get in the KNOW!
The premier event on identity and the data economy,
KNOW 2019 is expanding
to the ARIA Resort in Las Vegas March 24-27.
Enjoy leading-edge product demos, expert content sessions,
in-depth policy forums, and innovations in digital identity.
Take advantage of 10% of registration
with promo code:
PAYPERS10
www.knowconf.com
PRESENTED BY
ONE
WORLD
IDENTITY



Digital Identity at Border: Between Standardisation and Innovation

Consult Hyperion

Making Sense of Digital Identity

About Steve Pannifer: Steve is COO at Consult Hyperion and a digital identity and security expert. Steve has a detailed understanding of the global digital identity market having advised numerous organisations around the world on all aspects of digital identity – commercial, technical and regulatory. He is actively involved in key identity initiatives in both government and financial services sectors and is a regular speaker at digital identity conferences and events.

Steve Pannifer | *COO* | Consult Hyperion

Everyone is talking about digital identity

Individuals are becoming increasingly aware of the lack of control they have over their personal data, which is in effect what constitutes their digital identity. Banks are facing new regulatory requirements, such as 5AMLD and PSD2, making digital approaches identity an imperative. Other sectors such as health and employment are encountering identity-related issues as they seek to go digital. And there are numerous attempts at creating digital identity systems being made by governments and industry – all different, solving similar problems in different ways.

How can we make sense of it all?

Firstly, we need to understand what problem we are trying to solve.

Today identity is held in silos. Each organisation a customer interacts with has its own "virtual identity" for the customer, consisting of the personal information that the organisation needs. These virtual identities are locked up. If the customer wants to open a new bank account, buy insurance, submit his or her taxes and so on, the existence of these virtual identities does not help. Today customers have no way of saying "Look, my bank can tell you who I am".

Secondly, we need a model that helps us fix the problem. At Consult Hyperion we use this one:

Digital identity bridges the real and virtual

When a customer onboards to a new service, the service will need to establish that the customer is real and unique. This is what we call "***identification***".

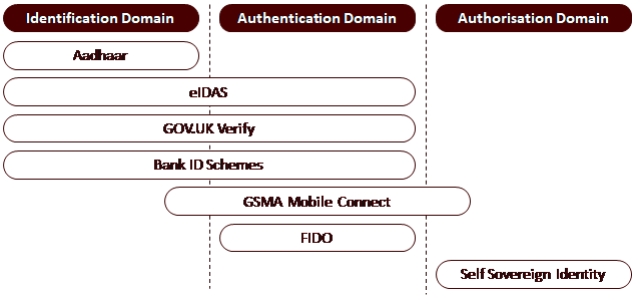
It is quite likely that the service will give the customer an app or ask them to set a password, allowing them to access that service more easily from that point forward. This is what we call "authentication" – asserting that the user is a previously established real customer.

The customer should then be given control over how their information (ie their virtual identity) is used. This is what we call "***authorisation***". Unfortunately, today this too often just boils down to giving marketing preferences. It should be much more than that. A customer should be able to say "Yes, please help me access that other service by telling them you know me". →

The key to creating portable virtual identities is the authentication domain in the middle. A customer should be able to present information signed by one organisation (a "claim") to another organisation and use their authentication method to show digitally that the claim belongs to them. This is how you would allow someone to digitally say "Look, my bank can tell you who I am".

Digital identity is the bridge between real identities and virtual identities. It is the means through which a person or an organisation can make their virtual identities portable.

Solutions that solve particular problems



The digital identity solutions that have been developed to date have solved particular problems.

India's Aadhaar programme is fundamentally about creating a register of real identities. In that sense, it is not really a digital identity system but was intended as a foundational step towards inclusion. Mainly, the widely reported issues with Aadhaar arise from the ways in which the register has subsequently been connected to digital identity systems.

eIDAS, GOV.UK Verify, and the successful Nordic Bank ID schemes all solve the narrow but important problem of allowing people to create and assert a digital version of their real identity. They do not, in their current forms, solve the wider need for portable virtual identities.

The GSMA has focused more on authentication, as that is the primary place mobile operators can play. FIDO provides similar but over-the-top device-based authentication.

consult hyperion
securing tomorrow's transactions

About Consult Hyperion: Consult Hyperion is an independent consultancy. We hold a key position at the forefront of innovation and the future of transactions technology, identity, and payments. We are globally recognised as thought leaders and experts in the areas of mobile, identity, contactless and NFC payments, EMV, and ticketing.

www.chyp.com

The various Self Sovereign Identity projects are about giving people total control over their virtual identities; but to work, people will need to be given tools in the authentication domain (eg wallets) to protect the keys that unlock those virtual identities.

Making it work for everyone

A key barrier to the adoption of digital identity solutions has been the perception (and in some cases the reality) that it will disrupt the relationship with the customer. Most solutions to digital identity today involve an "Identity Provider" that could equally be described as an "Identity Disintermediator". Instead of mobilising virtual identities, they create a new silo of data that sits between the customer and service. No service provider wants this.

In order to work, digital identity needs to be a low-cost enabler that is focused on providing the customer with the ability to move seamlessly (and securely) from one digital service to another. Until this is widely understood we will continue to have fragmented solutions with narrow applicability and limited adoption.

EEMA

eIDAS – Its Role in Our Future

About Jon Shamah: Jon Shamah is the Chair of EEMA. He is a recognised international Digital Identity & Trust Subject Matter Expert, specialising in maximising the operational value chain of national eID schemes. He is a frequent public speaker on issues regarding identity, Trust and EU Trust Services regulations, and he contributes to European Programs such as FutureTrust and LIGHTest.

Jon Shamah | *Chair* | EEMA

Imagine a world where citizens of the European Union can travel, work, and live wherever they choose, regardless of their native country. A place where you can transact with any EU bank or other financial institutions; where you can keep your original records of your pensions, savings, health data, no matter where they were initially created.

This is the goal of building The Single Digital Society envisioned by the EU, for which the first big steps have already been taken. Those steps are an assembly of identity, trust, data protection, and finance measures helping both citizens and business to achieve the EU's vision of a Single Digital Society.

Arguably, the **eIDAS Trust Services Regulation** is the most important of these measures. This regulation, which is an applicable law in all Member States, brings a "level playing field" across the entire EU to identity recognition, digital signatures, company seals, and other related services. It also enables digital legally admissible registered email services.

Simply, identity credentials that are accepted in one Member State for authentication in order to access government services must be recognised in all Member States for similar government services, if they are declared ("Notified") to the EU by that Member State.

Similarly, high confidence Qualified Digital Signatures (which require face-to-face enrolment) issued by a Qualified Trust Services Provider (QTSP), whether a person or a corporate, will be legally admissible across the entire EU. Know Your Customer (KYC) is also simplified by eIDAS; thus, by using a "Notified eID", the process can be conducted almost entirely online.

So what does this mean for a business?

Digital Transformation has been proven to be a major source of cost and time savings when applied to workflows and processes in business. This is particularly obvious in the Financial Services sector, where many products and services require legally binding agreements by all parties. A typical example may be represented by the application and provision of a mortgage or loan.

Digital Transformation of these workflows and digital signing of complex documents can save substantial amounts, but until now they have traditionally been restricted to the home Member State and its citizens, mainly for reasons regarding legal admissibility and KYC compliance. This limits the potential market.

eIDAS can bring strong benefits. Qualified eIDAS signatures are legally admissible across the entire EU, and most citizens can use the signing certificate in their National eIDs. This means that, with little additional effort, market size can be significantly increased, and so the Return on Investment for digitisation can be really improved with little extra risk. This applies even better to organisations that have responsibilities distributed across many countries. ➔

The relation with PSD2 and SEPA

eIDAS is also specified as the identification scheme used in the new **Payment Services Directive** (PSD2). This disruptive Directive brings the prospect of permissioned direct access to end-user bank accounts. Third Party Provider Financial Services companies (TPPs) can now offer a whole range of services that were previously not possible without breaches of security. For example, before PSD2, if an end-user wished to obtain a single consolidated view of his financial status, across many financial institutions, the end user would have been forced to provide the account aggregator with the account numbers and password. Not only was this very much frowned upon, and an obvious risk, but there was also no possibility of an audit trail as essentially the aggregator was logging in as the end-user. Now, with PSD2, the TPP will be able to view and alter the account within the parameters permissioned by the end-user.

This does require a high degree of certainty of the identity of the end-user and their consent to actions, as well as the certainty that the entire process is originating from the known and correct TPP.

PSD2 calls for the possibility of accessing customer account information, to initiate payments on behalf of the customers, and this access to be based on Strong Customer Authentication (SCA).

Qualified Certificates (QWACs) for Websites and Qualified Certificates for Electronic Seals (issued by Qualified Trust Service Providers) will enable the identification and the verification of the payment institution by a third party. This process will use identification based upon the legal name of an organisation, its registration number, and its primary role in the transaction.

The Single European Payment Area (SEPA) calls for European-wide payment mandates, in which "The creditor may offer the Debtor an automated means of completing the mandate, including the use of an electronic signature." Typical uses are regular bill payments, credit agreements, etc.

A Qualified Digital Signature issued by a Qualified Trusted Service Provider (QTSP), being legally admissible across the EU, is the ideal vehicle for this certainty across the EU and is seen as a major component of SEPA. The result is the capability to set up a regular payment mandate to fulfil any cross-border transaction or service provision.

About EEMA: EEMA is a leading, not for profit, independent European think tank including topics on Identification, authentication, privacy, risk management, cybersecurity, the Internet of Things, artificial intelligence, and mobile applications. EEMA helps organisations to maintain their competitive edge through projects, world class events, and Pan-European business networking at the highest levels.

www.eema.org

In summary, eIDAS will quickly become an integral regulation in our financial lives and an enabler, making the Single Digital Society a practical reality for European Financial Services.

Further information on eIDAS can be found at: **https://ec.europa.eu/digital-single-market/en/discover-eidas**

Innovate Identity

Self-Sovereign Identity and Shared Ledger Technologies

About Ewan Willars: Ewan is a senior associate with Innovate Identity. In recent months, he has undertaken digital identity market analysis for several national and international clients in the airline and banking sectors, and currently sits on both the UK Civil Aviation Authority's future's group, and the UK Fintech Delivery Panel.

Ewan Willars | *Senior Associate* | Innovate Identity

A vanguard of a bright new digital identity world, or an over-hyped innovation?

The digital identity industry worldwide has been subjected to a series of over-hyped innovations – new technology and new approaches that each promise to be the vanguard of a bright new digital identity world, but seldom deliver on the hype. This leaves senior decision makers unsure what to believe, and whether substance lies beneath the perennial excitement of innovation.

The latest approaches to emerge have been the concepts of *self-sovereign identity* (where you control your personal identity data locally, often on a device and with a personal key of some kind) and shared *ledger technologies* (where a common digital ledger of transactions and data is updated across all the scheme users). Both individually, and applied collectively, they have generated huge conversation and excitement.

But what evidence suggests that these approaches may succeed, when so many others have fallen by the wayside?

The moment feels right for self-sovereign

Self-sovereign feels like an approach that is emerging at the right time. Whether born by the new move towards providing people with better control over their personal data or merely in alignment by chance, self-sovereign feels very 'of the moment'.

When the hype is carefully peeled back, the natural alignment between a self-sovereign approach and the recent direction of data protection regulation is laid clear, with both providing for individuals to have greater control over how and when their personal data is used. Self-sovereign is a child of its time, and as such its relevance can't be easily ignored.

Shared ledger technology can unlock the potential of self-sovereign

Self-sovereign, as a concept, is blind to technology. However, the synergy between shared ledger approaches and the self-sovereign ethos is readily apparent. Neither self-sovereign nor shared ledgers are dependent on each other; other forms of personal attribute storage and transmission are available.

However, the ability of self-sovereign and shared ledger combined to maintain a common, trusted record of attributes and events, putting users in direct control of their personal identity data, and simultaneously removing the need for large central entities to provide the attribute exchange is a potent and perhaps unique combination.

Self-sovereign and shared ledger are fast emerging as credible ways to assist those suffering identity challenges

The lack of a means to demonstrate one's identity, to assert who you are at crucial times, is a major issue around the world for a billion people or more. The **UN Sustainable Development Goals seek to ensure a legal identity is available to all by 2030**; digital identity is one (perhaps significant) means to achieve that goal. ➔

Providing every individual with a way to demonstrate their identity would be a big step forward. In particular, the shared ledger approach, where individuals can 'build' a trusted identity over time, even in the absence of traditional identity credentials, is a potentially very positive development.

Overall, the positives may outweigh the negatives, but significant barriers to adoption still remain

✓ Self-sovereign and shared ledger approaches could be used across a wide range of relying parties and for a huge variety of uses, given the right regulation and commercial models.

✓ Self-sovereign has great potential to reduce the growing regulatory burden, recently created by the consent regimes of GDPR and other personal data regulation.

✓ The use of shared ledgers can build a unique identity even for those with no access to more traditional and formal means of identifying themselves.

X The current deployments often lack interoperability. This reflects the lack of commonly accepted standards and serves to fragment the market.

X A lack of regulatory certainty creates market uncertainty and a barrier to adoption, particularly for highly regulated industries such as financial services.

X Digital identity schemes need both attribute providers and relying parties within their trust framework, with banks often playing a part in both roles. Self-sovereign schemes do not start with a 'ready-made' roster of relying parties – and without a sufficient level of utility for the end user, digital identity schemes of any design are doomed to failure.

? An unanswered question at this stage is whether a significant number of individuals actually want (or even have the capacity) to manage their personal data themselves. The future of self-sovereign identity solutions depends on the appetite and adoption of users.

What next?

It is too early to reasonably predict the future success or otherwise of the self-sovereign approach. However, the principles it places at the heart of the approach – recording consent and what transactions take place, enabling the individual's control over their personal data, empowering the individual to call forth their own identity attributes – accurately reflect digital identity challenges today.

About Innovate Identity: Innovate Identity is an independent consultancy providing advisory services focused on digital trust, data and technology innovation within the global online community. Our areas of expertise include global identity proofing, 'Midata', identity verification, age verification, Know Your Customer, anti-money laundering, data privacy, and anti-fraud technologies. We improve our client's global reach, competitive advantage, return on investment, and we enable sustainable business transformation through identity innovation.

www.innovateidentity.com

However, as with shared ledger, there needs to be further exploration and test deployments. Regulators, in particular, need to demonstrate their understanding and create a path for innovation to flow to the market. Industry 'sandboxes', such as that introduced by the UK Financial Conduct Authority, are a positive development, somewhat de-risking the testing of new solutions. They also allow regulators to consider new approaches in practice, how they might be appropriately regulated, and the potential need for new industry standards.

While in practice neither self-sovereign nor shared ledgers provide a general panacea for identity, both approaches have hugely exciting potential, particularly when combined. But, ultimately, only the identity market will decide if they will achieve the widespread adoption needed to deliver on their undoubted promise.

The Regulatory Space

DALIR

A Brief Summary of EBA Guidelines on Fraud Reporting Under the PSD2

About Irena Dajkovic : Dr Irena Dajkovic is a lawyer with a combination of about twenty years of private practice and in-house experience in commercial, corporate, and regulatory laws. Over the years, her clients ranged from financial institutions, private equity firms, retail companies to private individuals. She focuses on clients' goals and has often been praised by them for her excellent technical skills, strategic advice, and high ethical standards.

Irena Dajkovic | *Partner* | DALIR

Article 96 (6) of the revised Payment Services Directive EU 2015/2366 (PSD2) requires Member States of the European Union to ensure that payment service providers (PSPs) provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities are also required to provide the European Banking Authority (EBA) and the European Central Bank (ECB) with such data in an aggregated form. Based on this, the EBA had previously drafted Guidelines on Fraud Reporting under the PSD2 and had consulted on it earlier in 2017. On 18 July 2018, EBA issued a report with the final Guidelines on Fraud Reporting under the PSD2 (the Fraud Guidelines).

When will the Fraud Guidelines come into force?

Data collection is set to begin on 1 January 2019, except for required data breakdowns on the usage of exemptions from the secure customer authentication (SCA) requirement, for which data collection will begin once the Regulatory Technical Standards on SCA and CSC (the RTS) come into force on 14 September 2019.

Who do the Fraud Guidelines apply to?

The EBA actually developed two sets of guidelines: the first set is addressed to the PSPs and the second set applies to the Member States' competent authorities (CAs) tasked with providing the fraud reporting data to the EBA and the ECB. Article 96 (6) stipulates that PSPs must provide statistical data on fraud relating to different means of payment, without explicitly excluding any particular type of PSPs. However, the EBA has clarified that Account Information Service Providers (AISPs) are out of the scope of the fraud reporting requirements. AISPs are PSPs that simply offer consolidated information on a user's different payment accounts, and as such cannot report any fraudulent payment transactions data, thus the EBA concluded that including them would require changing the scope of the Fraud Guidelines.

What must be reported?

In the original draft Guidelines, the EBA proposed to require reporting under three broad categories: "unauthorised transactions", "manipulation of the payer", and "payer acting fraudulently". In the final Fraud Guidelines, the EBA narrowed it down to two, and eliminated the "payer acting fraudulently" category, following a number of complaints from respondents to the draft Guidelines. The reasoning of the respondents, subsequently adopted by the EBA, is that fraudulent payers are completely outside the control of the PSPs, and data on such fraud is of limited value to supervisors, because PSPs cannot identify when the payer itself is acting fraudulently through their transaction risk monitoring systems. On the other hand, respondents also wanted the EBA to eliminate the "manipulation of the payer" category, but the EBA decided against this. EBA reasoned that the category is important because PSPs have the responsibility to adopt measures to detect where payers are potentially being scammed. →

How must the data be reported?

The aforementioned categories are further divided into data breakdowns, depending on the type of payment service (e.g., direct debit, money remittance or credit transfer), payment instrument (e.g., e-money or card), and relevant reporting PSP (whether card-payment transactions are reported by the issuer or acquirer). Furthermore, although the draft Guidelines posited the possibility that PSPs would have to provide a breakdown on a country by country basis, a number of respondents considered this requirement too onerous, and the EBA concluded that there was no strong need for country-by-country data. Consequently, the final Fraud Guidelines only require PSPs to report transaction data according to whether they are domestic, cross-border transactions within the EEA, or cross-border transactions outside the EEA.

How often must data be reported?

Article 96 (6) requires PSPs to provide the statistical data on fraud at least annually. In the draft Guidelines, the EBA first proposed reporting the data sets on a quarterly basis. However, the EBA's proposal was subject to criticism by many respondents due to the administrative burden of quarterly reporting. Taking that into consideration, the EBA concluded in the final Fraud Guidelines that the data should be provided on a semi-annual basis instead. Additionally, the EBA established an exception to the rule for small payment institutions and e-money institutions, who would only have to provide the data on an annual basis with a semi-annual breakdown.

The overlap with the fraud monitoring requirement under the RTS on SCA and CSC

In order to make use of the exemptions from conducting secure customer authentication in the RTS, Article 21 of the RTS requires PSPs to conduct quarterly fraud monitoring, which must be made available to competent authorities and the EBA at their request. Many PSPs questioned what the overlap was between this requirement in the RTS and the fraud reporting requirement under Article 96 (6). Subsequently, in its June 2018 Opinion on the Implementation of the RTS, the EBA stated that the fraud rate calculated under Article 21 would have to include the same categories of fraud as the Fraud Guidelines ("unauthorised transactions" and "manipulation of the payer"). Of course, this does not mean there is total overlap between the two.

While companies must conduct quarterly monitoring under Article 21, their reporting duty under the Fraud Guidelines is semi-annual. Furthermore, while Article 21's data breakdowns are concentrated on whether the transactions were SCA-exempted or not, and what exemption was used, the final Fraud Guidelines require much more, as we have detailed above. However, undoubtedly, PSPs will see some overlap in the data categories collected and will be able to leverage this for their compliance needs.

Disclaimer: This article does not necessarily deal with every important aspect nor cover every detail of the topic it discusses. It is not designed to provide legal or other advice.

Timelex

Reconciling Consent in PSD2 and GDPR

About Niels Vandezande: Niels Vandezande is a legal consultant at Timelex. He previously worked as postdoctoral researcher at the KU Leuven Centre for IT & IP Law. Niels specialises in fintech, more particularly in virtual currencies, electronic money, payment services, and blockchain.

Niels Vandezande | *Legal Consultant* | Timelex

The Second Payment Services Directive **(PSD2)** adds third-party payment service providers – particularly account information service providers (AISP) and payment initiation service providers (PISP) – to the EU's legal framework on payment services. This means that traditional payment service providers will need to share certain data with those third-party providers. Much of that data will be very personal in nature and may constitute personal data in the sense of the EU's data protection framework set by the General Data Protection Regulation **(GDPR)**. This results in friction between being required to share personal data and at the same time being required to conduct such sharing under very strict conditions, resulting in a compliance conundrum. Even after the entry into force of both legal frameworks, several uncertainties remain. In this article, we look at one particular matter, namely that of explicit consent, and the guidance provided in this matter by the **European Data Protection Board** (EDPB).

Data sharing under PSD2

PSD2's article 67 provides the rules on access to and use of payment account information in the case of account information services. This article gives payment service users the right to make use of services, enabling them access to account information. Account information service providers, however, can only provide their services based on the payment service user's explicit consent. They may only access the information from designated payment accounts and associated payment transactions, they may not request sensitive payment data linked to those accounts, and they may not use, access, or store any data for purposes other than for performing the service explicitly requested by the user.

Similarly, according to article 66, a payment initiation service provider may only provide its services on explicit consent. Also, they may not request any data other than those necessary to provide their services, and may not use, access, or store any data for purposes other than for the provision of the service as explicitly requested by the payer.

Article 94 of PSD2 provides the data protection standard of this legal framework, considering that payment service providers shall only access, process, and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user. Moreover, all personal data processing in the context of PSD2 must be compliant with the EU's data protection framework, now set by GDPR.

Consent under GDPR

Under the EU's data protection framework, personal data may only be processed under a limited number of lawful grounds (article 6 GDPR). These include six types of processing:

- processing under the data subject's consent,
- processing necessary for contractual obligations,
- processing necessary under statutory obligations,
- processing necessary for the protection of the vital interests of the data subject,
- processing necessary for a task performed in the public interest, and
- processing necessary in the legitimate interests of the data controller. ➔

Regarding consent, the GDPR's article 7 provides that the data controller must be able to demonstrate that consent was freely given. Consent for one matter must be distinguishable from other matters, and consent may be withdrawn at any time. When processing a child's information – up to ages between 13 and 16, depending on the Member State – consent must be given or authorised by the holder of parental responsibility. When processing special categories of personal data – such as racial origin, political leanings, or health data – consent must be explicit.

This shows that both GDPR and PSD2 use a notion of consent, or even explicit consent, even though the meanings do not seem to perfectly overlap. Moreover, it can be questioned whether explicit consent is really needed if it can be argued that the processing of the payer's personal data by a third-party payment service provider is necessary for the fulfilment of a contract between them – i.e. to provide a payment initiation or account information service. The presence of that lawful ground means that under GDPR no consent would be needed – as consent is a different lawful ground – even though PSD2 still requires explicit consent.

EDPB guidance

The EDPB provided some **guidance** on the matter in July 2018.

It confirms that third-party payment services provide their services based on a contract between them and the payment service user, in accordance with recital 87 PSD2. This means that for personal data processing in this relationship under GDPR, the lawful ground of contractual necessity can indeed apply. Contractual clauses – distinct from other contractual matters – should then specify the purposes for which the user's personal data will be processed, to which the user should explicitly agree. The explicit consent mentioned in PSD2 should be seen as an additional requirement, separate from the requirements following from GDPR. Explicit consent under PSD2 is, therefore, a contractual consent, and not a data processing consent.

Conclusion

The EDPB's guidance is the first assessment of some of the issues resulting from the interplay between PSD2 and GDPR. While the guidance is not exhaustive, and some issues certainly remain, it does provide a welcomed clarification that the notion of explicit consent under PSD2 must be seen as separate and different from the notion of (explicit) consent under GDPR. Moreover, it allows for the processing of personal data to be seen under GDPR's lawful ground of contractual necessity, rather than imposing the lawful ground of consent in this matter. This makes consent under PSD2 more of a transparency requirement (what data are processed and why), rather than being bound to the stricter requirements of consent under GDPR.

About Timelex: Timelex is a law firm specialised in fintech, information, and technology law in the broadest sense, including privacy protection, data, and information management, e-business, intellectual property, online media, and telecommunications.

www.timelex.eu

Payment Counsel

Bitcoin and AML: Regulating the New Mainstream

About Nadja van der Veer: Nadja van der Veer is a payments lawyer with almost 10 years of experience in the international Payments industry and a legal expert in rules and regulations involving PSD, AML and CDD, and Card Schemes. As Co-Founder of **PaymentCounsel** and one of the Managing Partners of **Pytch Ventures**, she consults Merchant Acquirers, Payment Services Providers (PSPs/MSPs), other Fintech companies, and Merchants in their startup phases who want to expand their business internationally, while mitigating risk.

Nadja van der Veer | *Co-Founder* | Payment Counsel

Cryptocurrency has been historically involved in a lot of negative news, instigated by government warnings. Governments have raised concerns relating to its price volatility, anonymity, and its association with the dark web. The European Supervisory Authorities (ESAs) have come up with a whole list of risks, including lack of exit options and lack of price transparency. However, benefits to cryptocurrency are also being acknowledged. It can improve payment efficiency, reduce transaction cost, it is cheaper, faster, and more secure. It addresses the needs of the unbanked and it is irreversible.

Regulatory attempts

The regulatory attempts made worldwide lack a consistent and unilateral approach. Some jurisdictions went for a separate licensing system, others chose putting AML obligations on cryptocurrency service providers. While others use an existing licensing system like e-money or class it as a defined asset, others feel that since cryptocurrencies are not created or controlled by any central entity, that any applicable financial industry regulations are not suitable. It is important to know that if regulators choose one of these options they must carefully balance these to ensure that it does not stifle innovation.

Be ready for 5AMLD

While certain crypto exchange platforms have already voluntarily been applying identification and verification of their customers in order to fulfil demands of banking partners (or to disassociate themselves from the criminal use of cryptocurrency) now, in order to keep pace with technological innovation, the European Commission has put cryptocurrency exchange platforms and custodian wallet providers into the scope of the EU AML Directive (5AMLD). Since the 5AMLD refers to virtual currency, we will keep this reference, but cryptocurrency has been given many more names. The main reasons for the AMLD change are related to concerns that these exchange platforms have no legal obligation to identify suspicious activity and that the anonymity aspect of virtual currency (VC) allows potential misuse for criminal purposes.

The Commission has chosen a broad application of virtual currency purposes as being a means of payment, exchange, for investment purposes, as store-of-value products, or for use in online casinos. While the definition of VC exchange platforms is quite obvious and speaks for itself (parties that exchange between VC and fiat currency), the definition of custodian wallet providers seems still a bit ambiguous and perhaps too broad. They are 'an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store, and transfer virtual currencies.' Potentially, this has the consequence that parties which are not really designed as wallets but hold private keys may fall under the Directive as well. And what about multisig key holders, which could be individuals? But they won't have the capabilities to comply with the Directive and they shouldn't. ➔

How would they be able to identify the transaction as being suspicious? Including parties like this can stifle the development and innovation ongoing, so this broad definition is not always supported throughout the industry.

The ambiguous definition is perhaps the result of the European Commission also not really knowing where the market and technology are going to, or – even worse – not really understanding the underlying principles of VC.

As all other obliged entities, VC exchange platforms and custodian wallet providers will need to comply with all AML obligations, from identification to verification, to ongoing monitoring to suspicious activity reporting. While the initial draft proposals were setting licensing requirements to these new obliged entities, this has now been transformed into a registration condition. The 5AMLD must be implemented into national laws by 10 January 2020. VC exchange platforms will have to watch regulators' actions closely as more countries (especially APAC) are adapting their anti-money laundering regulations to include VC platforms.

Are the concerns real and the measures effective?

The **UK House of Commons Twenty-Second Report of Session 2017-2019** on Crypto-assets also recognised the risk of cryptocurrencies (according to stakeholders questioned for the report, crypto-assets is a more appropriate terminology) acting as a vehicle for money laundering. However, it is interesting to note that the UK National Crime Agency in its latest risk assessment has determined that the use of cryptocurrency for money laundering and terrorist financing is currently low. Cases are present, but it is not widespread. Placing this into context, the NCA stated that there are other large-scale areas of the money laundering problem over cryptocurrency. Quite interestingly, HM Treasury has explained that certain characteristics of cryptocurrency in fact disincentive criminals from using them to launder money: while cryptocurrency is 'an anonymous way of paying for illicit activity, there is the fact that you are potentially creating a more transparent record of the transaction, which is potentially auditable… There are other methods available to them [terrorists], many of which are easier, such as cash couriers", the House of Commons Report continues.

Further concerns about the effectiveness of the changes in combating money laundering and terrorist financing relate to the aim of the 5AMLD to ensure traceability of VC and to lift anonymity. However, the Commission also fully acknowledges that a large part of the VC environment will remain anonymous because transactions can also take place without exchange platforms or custodian wallet providers. We are yet to see if these changes will have a true impact.

Perhaps the industry doesn't really need any more regulatory changes, but rather requires more focus on collaboration (not only between member states but also between obliged entities) and on how the obligations are to be fulfilled. Regardless, the 5AMLD is there and the changes seem to be welcomed by the industry as the lack of regulation would still mean that especially the fiat to crypto conversion and vice versa is vulnerable to criminal activity, as stated by CryptoUK.

TRUSTECH
Digital | Trust | Technologies














THE LEADING EVENT

FOR DIGITAL TRUST TECHNOLOGIES

#TRUSTECH2018

REGISTER ONLINE

www.trustech-event.com

27 › 29 Nov.

Palais des Festivals
Cannes France

2018

COMEXPOSIUM

Fraud Detection, Identity Verification & Online Authentication – Mapping and Infographic

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Anda Kania | *Senior Editor* | The Paypers

The industry's spectrum

If we look at the security and fraud issues in the financial and payments sector today, try as one might, the online environment is still vulnerable, despite the efforts made to combat fraud. This is due, in part, to the growth of digital commerce and digital banking channels. According to Gemalto's **Breach Level Index**, more than 2.5 billion records were stolen or compromised in 2017, with identity theft as the leading type of data breach. On the same note, the **2018 Global Fraud Trend Analysis and Review** of CMSPI and MAG has revealed that growth in the card payments market and increased CNP transactions continue to provide fraudsters with opportunities. The fact that fraudsters are digging for new ways of outsmarting the security systems and protocols is not outstanding, of course; however, it is interesting to see the way they shift focus from credit card data to account data or the way they combine social engineering skills with technical ones.

Fraud has become an extremely visible challenge for both merchants and banks. A **TransUnion study** has revealed that 94% of financial services have experienced fraud within the last two years, such as identity theft, synthetic identity fraud or account takeover. The latter is also giving a hard time to merchants and their customers, along with chargebacks, MOTO fraud, BOPIS fraud, telecomm fraud and many more. At the same time, the industry players must be disruptive; they need to find ways to reduce fraud and operational costs, enhance customer experience, meet regulatory needs and be as dynamic as the market is. With challenger banks and tough competition in all online verticals - from retail, to digital and travel - effective fraud management is becoming a competitive advantage.

Hence, solution providers constantly add new capabilities through product improvements, partnerships and acquisitions. For example, RELX Group has acquired ThreatMetrix to ramp up their risk-based authentication capability. Furthermore, payment companies integrate fraud capabilities in their solutions, like PayPal did by acquiring Simility, or Emergent Technology by acquiring Trust Stamp.

In order to create an accurate picture of what the fraud detection, identity verification and online authentication offerings look like, we have decided to display the key players of the industry together with their main capabilities. Depicting the most important features of each company is part of our goal of helping merchants, banks, fintechs and payment service providers to grasp the current market's opportunities and to use them according to their own needs.

The fraud management section delineates the main relevant features of solutions providers, such as stateless data ingestion and augmentation (which is the ability to ingest all types of data, structured, unstructured, third party, user as well as device/ behavioural biometrics), supervised and unsupervised ML, intelligence, case management, orchestration layer, adaptive decisioning and many more. These intelligent and advanced technologies of using advanced data analytics and ML to identify fraud has been gathering momentum for some time. The whole range of capabilities is designed to address the pain points that organisations in the payments space are struggling to remove. Payment fraud, account takeover, friendly fraud, identity theft, CNP fraud, new account fraud and whatnot are a few types of fraud that vendors featured in our mapping can prevent. ➔

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

As regards the digital identity verification, the application of machine learning analytics is essential to making sense of the data and approaching the challenge of achieving adequate risk and compliance objectives while ensuring a seamless customer experience across channels. Identity verification is a key component of the Know Your Customer, a process that financial institutions must conduct when onboarding customers. This includes the deployment of identity management and authentication techniques. The challenge appears when a bank or other type of financial services body chooses to expand in another country or another region, which applies different rules of due diligence.

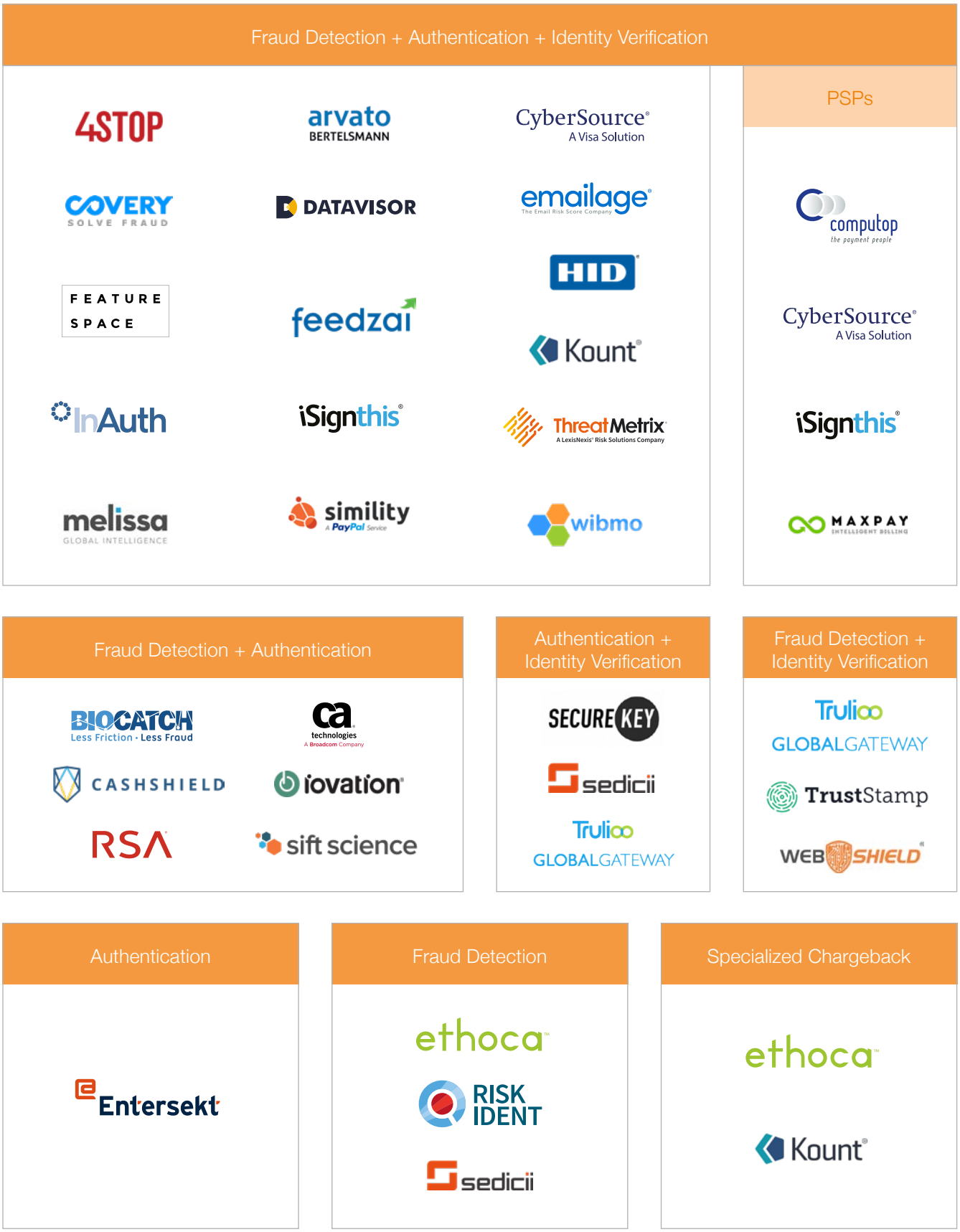
Various sectors such as financial services or ecommerce verticals (e.g. airlines, gaming, retail, etc.) are still dealing with authentication issues, as they look to provide digital access to locations and services, authorise payments, manage fraud, and stay compliant with different regulations around the world. For this reason, the online authentication section seeks to provide information related to biometrics and other authentication means that can assist organisations in achieving their goals of meeting compliance and the customers' expectations.

Some of the companies illustrated in the below mapping are offering an integrated package, while others are focusing on delivering niched solutions. For instance, Feedzai, Kount, Simility, or Featurespace offer services included in all three categories. We also notice payment services providers, such as Computop or CyberSource, integrating anti-fraud tools within their platform. There are companies that offer solutions under a single category, like SecureKey, which aims its attention at digital identity, or Entersekt, which is mostly focused on authentication.

Nevertheless, chances are that all anti-fraud, digital identity verification and authentication capabilities would merge even more in the upcoming years. Fraud detection, identity verification and online authentication are, of course, not the same thing, but they have one goal: to protect the businesses and consumers. In different ways, with different strategies, but in the end, how long it will take to fully intertwine?

Watch this space.

Fraud Detection, Identity Verification & Online Authentication – Infographic



Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	4STOP	arvato BERTELSMANN	BIOCATCH Less Friction · Less Fraud	ca technologies A Broadcom Company	CASHSHIELD
FRAUD DETECTION					
Target group					
Banks	x	x	x	x	x
Ecommerce/merchants	x	x		x	x
Acquirers/PSPs	x	x		x	
Fintech	x	x		x	
Technology					
On-premises	x	x			
Cloud-based	x	x	x	x	x
Hybrid	x	x			
Methodology					
Rule-Based	x	x	x	x	
Machine Learning		x	x	x	x
Hybrid	x	x	x	x	
Data Ingestion					
Stateless Data ingestion and Augmentation	x	x		x	x
Machine Learning					
Supervised learning	x	x	x	x	x
Unsupervised learning		x	x	x	x
Intelligence					
Abuse List	x	x	x	x	x
Monitoring	x	x	x	x	x
Address Verification	x	x			x
Credit Bureau	x	x			
Information Sharing Network	x	x		x	x
Case management	x	x	x	x	
Manual review	x	x		x	
Orchestration layer		x		x	
Adaptive decisioning		x		x	x
Chargeback management	x				
Recovery	x		x		
Guaranteed fraud prevention	x				x

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	4STOP	arvato BERTELSMANN	BIOCATCH Less Friction · Less Fraud	ca technologies A Broadcom Company	CASHSHIELD
IDENTITY VERIFICATION					
ID verification	x				
Identity Document Scanning	x				
Video scanning					
Personally identifiable information (PII) Validation	x	x			
Derived verification	x	x			
Small Transaction verification	x				x
Email verification	x				
Phone verification	x				
Social verification	x				
Additional checks/compliances	x				
Credit check	x	x			
Compliance check	x				
AUTHENTICATION					
Behavioural biometrics			x		
Session analysis		x	x	x	x
Device-user interaction		x	x	x	x
Physical biometrics					
2-D facial recognition				x	
Voice				x	
Fingerprint scan				x	
Iris scan					
Other					
Device fingerprinting	x	x	x	x	x
Geo-location	x	x	x	x	x
Remote access detection	x	x	x		x
Mobile app push				x	x
3-D secure 2.0		x		x	
Hardware token	x				
One-time passwords	x		x	x	x
Knowledge-Based Authentication	x	x	x	x	x

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	4STOP	arvato BERTELSMANN	BIOCATCH Less Friction · Less Fraud	ca technologies A Broadcom Company	CASHSHIELD
Customer Reference	Client Integrations: Mifinity Gatehub PaySend Paymentz Ontology	Further details for case studies are/will be found here: https://finance.arvato.com/en/financial-solutions/fraud-detection.html	Further details for case studies are/will be found here: https://www.biocatch.com/resources/case-studies	For more information contact our Sales Director Graeme.Bullock@ca.com	Fraud management solution https://www.cashshield.com/case-studies/razer-store/
Supported Regions	Global	Global	-	Global	Global

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	computop	CyberSource	DATAVISOR	emailage	Entersekt
FRAUD DETECTION					
Target group					
Banks	x		x	x	x
Ecommerce/merchants	x	x	x	x	x
Acquirers/PSPs	x	x	x	x	x
Fintech				x	x
Technology					
On-premises	x		x		
Cloud-based		x	x	x	
Hybrid			x		
Methodology					
Rule-Based	x	x			
Machine Learning	x	x			
Hybrid	x	x	x	x	
Data Ingestion					
Stateless Data ingestion and Augmentation	x	x			
Machine Learning					
Supervised learning	x	x	x	x	
Unsupervised learning		x	x	x	
Intelligence					
Abuse List	x	x	x	x	
Monitoring	x	x	x	x	
Address Verification	x	x			
Credit Bureau	x				
Information Sharing Network	x	x	x	x	
Case management	x	x	x		
Manual review	x	x	x	x	
Orchestration layer		x	x	x	
Adaptive decisioning	x	x	x	x	
Chargeback management					
Recovery					
Guaranteed fraud prevention		x			

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	computop	CyberSource	DATAVISOR	emailage	Entersekt
IDENTITY VERIFICATION					
ID verification					
Identity Document Scanning					
Video scanning					
Personally identifiable information (PII) Validation		x		x	
Derived verification					
Small Transaction verification					
Email verification	x		x	x	
Phone verification			x	x	
Social verification	x		x	x	
Additional checks/compliances					
Credit check	x				
Compliance check					
AUTHENTICATION					
Behavioural biometrics				x	
Session analysis			x		
Device-user interaction		x	x		
Physical biometrics					
2-D facial recognition	x				x
Voice	x				
Fingerprint scan	x				x
Iris scan	x				x
Other					
Device fingerprinting	x	x	x		x
Geo-location	x	x	x	x	x
Remote access detection		x	x		x
Mobile app push		x			x
3-D secure 2.0	x	x		x	x
Hardware token	x				
One-time passwords	x	x			x
Knowledge-Based Authentication					

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	computop	CyberSource A Visa Solution	DATAVISOR	emailage	Entersekt
Customer Reference	Information upon request	GHD, Decision Manager https://www.youtube.com/watch?v=F6oi0YAQixc	More information upon request	OFX, Email-Risk Score: https://pages.emailage.com/rs/099-GUT-421/images/Emailage_CustomerStory_OFX_112118.pdf	Capitec Bank, push-based, in-app authentication as one-time password replacement ; Investec, push-based, in-app authentication as one-time password replacement,
Supported Regions	Europe The Americas China South-East Asia	North America Europe Middle East Africa Asia Pacific ATAM	US EMEA APAC	Global	North America Europe Middle East Africa

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	ethoca	FEATURE SPACE	feedzai	HID	Accertify InAuth
FRAUD DETECTION					
Target group					
Banks	x	x	x	x	x
Ecommerce/merchants	x	x	x		x
Acquirers/PSPs	x	x	x		x
Fintech			x	x	x
Technology					
On-premises		x	x	x	x
Cloud-based	x	x	x	x	x
Hybrid	x	x	x	x	
Methodology					
Rule-Based		x	x	x	x
Machine Learning		x	x	x	x
Hybrid		x	x	x	x
Data Ingestion					
Stateless Data ingestion and Augmentation		x	x	x	
Machine Learning					
Supervised learning		x	x	x	x
Unsupervised learning		x	x	x	x
Intelligence					
Abuse List		x	x	x	x
Monitoring		x	x	x	x
Address Verification			x		x
Credit Bureau		x	x		x
Information Sharing Network	x	x	x		x
Case management		x	x	x	
Manual review		x	x	x	x
Orchestration layer			x		x
Adaptive decisioning		x	x	x	x
Chargeback management	x				x
Recovery	x	x			
Guaranteed fraud prevention					

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	ethoca	FEATURE SPACE	feedzai	HID	Accertify InAuth
IDENTITY VERIFICATION					
ID verification					
Identity Document Scanning			x		
Video scanning					
Personally identifiable information (PII) Validation			x		x
Derived verification		x	x		
Small Transaction verification		x			
Email verification			x	x	x
Phone verification			x		x
Social verification			x		x
Additional checks/compliances					
Credit check		x	x		
Compliance check		x			
AUTHENTICATION					
Behavioural biometrics		x		x	
Session analysis		x	x	x	x
Device-user interaction		x	x	x	x
Physical biometrics					
2-D facial recognition				x	
Voice					
Fingerprint scan				x	x
Iris scan					
Other					
Device fingerprinting		x	x	x	x
Geo-location		x	x	x	x
Remote access detection			x	x	x
Mobile app push				x	x
3-D secure 2.0		x		x	x
Hardware token			x	x	
One-time passwords		x		x	
Knowledge-Based Authentication		x	x	x	

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	ethoca	FEATURE SPACE	feedzai	HID	Accertify InAuth
Customer Reference	Ethoca Alerts; EasyJet Airline	Worldpay, Machine learning risk management and fraud prevention platform	More information available upon request	More information upon request	Further details for Accertify case studies are/will be found here: https://www.accertify.com/en/resources/#CaseStudies
Supported Regions	US Europe Middle East Africa AsiaPac India China LATAM	US Europe Middle East Africa AsiaPac India China LATAM	Global	Global	North America LATAM Asia Pacific Europe Middle East Africa

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	iovation	iSignthis	Kount		melissa
FRAUD DETECTION					
Target group					
Banks	x	x	x	x	x
Ecommerce/merchants	x	x	x	x	x
Acquirers/PSPs	x	x	x	x	x
Fintech	x	x	x	x	x
Technology					
On-premises					
Cloud-based	x		x	x	x
Hybrid		x			
Methodology					
Rule-Based	x		x	x	
Machine Learning	x		x	x	
Hybrid	x	x	x	x	
Data Ingestion					
Stateless Data ingestion and Augmentation		x	x		
Machine Learning					
Supervised learning	x	x	x	x	
Unsupervised learning			x	x	
Intelligence					
Abuse List	x	x	x	x	x
Monitoring	x	x	x	x	
Address Verification		x	x	x	x
Credit Bureau				x	x
Information Sharing Network	x		x	x	
Case management			x		
Manual review		x	x	x	
Orchestration layer		x	x	x	
Adaptive decisioning			x	x	
Chargeback management		x	x		
Recovery			x		
Guaranteed fraud prevention					

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	iovation	iSignthis	Kount		melissa
IDENTITY VERIFICATION					
ID verification					x
Identity Document Scanning		x			
Video scanning		x			
Personally identifiable information (PII) Validation		x	x		x
Derived verification					
Small Transaction verification		x			
Email verification		x	x	x	x
Phone verification		x	x	x	x
Social verification				x	x
Additional checks/compliances					x
Credit check		x			
Compliance check		x	x		x
AUTHENTICATION					
Behavioural biometrics			x		
Session analysis		x	x	x	
Device-user interaction	x	x	x	x	
Physical biometrics					
2-D facial recognition	x				
Voice					
Fingerprint scan	x				
Iris scan					
Other					x
Device fingerprinting	x		x	x	
Geo-location	x	x	x	x	x
Remote access detection	x		x	x	
Mobile app push	x		x		
3-D secure 2.0		x			
Hardware token					
One-time passwords	x	x	x		
Knowledge-Based Authentication		x			

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	iovation	iSignthis	Kount		melissa GLOBAL INTELLIGENCE
Customer Reference	Ikano Bank, Fraud Prevention	For more information, please get in touch with our team sales@isignthis.com	BodyBuilding.com, Kount Complete; Jagex Games Studio, Kount Complete; The Vitamin Shoppe, Kount Complete; Leatherman, Kount Complete; JOANN Fabric and Craft Stores, Kount Complete	More information upon request	Z1 Motorsports, Personator World:car2go Metabank
Supported Regions	US Europe Middle East Africa AsiaPac India China LATAM	Global	US Europe Middle East Africa AsiaPac China LATAM	Global	Global

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	RISK IDENT	RSA	SECURE KEY	sedicii	sift science
FRAUD DETECTION					
Target group					
Banks	x	x		x	
Ecommerce/merchants	x	x		x	x
Acquirers/PSPs	x	x		x	x
Fintech		x		x	x
Technology					
On-premises	x	x			
Cloud-based	x	x		x	x
Hybrid	x		x	x	
Methodology					
Rule-Based	x	x	x	x	x
Machine Learning	x	x	x	x	x
Hybrid	x	x	x	x	x
Data Ingestion					
Stateless Data ingestion and Augmentation		x			x
Machine Learning					
Supervised learning		x		x	x
Unsupervised learning		x			
Intelligence					
Abuse List	x	x			
Monitoring	x	x		x	x
Address Verification	x			x	
Credit Bureau	x		x		
Information Sharing Network	x	x	x	x	x
Case management			x		x
Manual review		x		x	x
Orchestration layer			x	x	x
Adaptive decisioning		x		x	x
Chargeback management					
Recovery					
Guaranteed fraud prevention					

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	RISK IDENT	RSA	SECURE KEY	sedicii	sift science
IDENTITY VERIFICATION					
ID verification					
Identity Document Scanning			x	x	
Video scanning			x	x	
Personally identifiable information (PII) Validation			x	x	
Derived verification			x		
Small Transaction verification			x		
Email verification			x	x	
Phone verification			x	x	
Social verification			x	x	
Additional checks/compliances			x	x	
Credit check			x	x	
Compliance check			x	x	
AUTHENTICATION					
Behavioural biometrics					
Session analysis			x		x
Device-user interaction			x		x
Physical biometrics			x		
2-D facial recognition		x	x	x	
Voice		x	x		
Fingerprint scan		x	x		
Iris scan		x	x		
Other					
Device fingerprinting		x	x	x	x
Geo-location		x	x	x	x
Remote access detection		x			
Mobile app push		x	x	x	
3-D secure 2.0		x			
Hardware token		x			
One-time passwords		x	x		
Knowledge-Based Authentication		x	x		

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	RISK IDENT	RSA	SECURE KEY	sedicii	sift science
Customer Reference	Please see customer references at https://riskident.com/en/	For more information, visit rsa.com/en-us/customers	More information upon request	More information upon request	Airbnb, Twitter Wayfair Yelp! Jet.com Remitly OpenTable Indeed Zoosk Instacart Everlane Patreon
Supported Regions	Europe US	Global	Global	Global	Global

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	similityA PayPal Service	ThreatMetrixA LexisNexis® Risk Solutions Company	TrustStamp	Trulioo
FRAUD DETECTION				
Target group				
Banks	x	x	x	x
Ecommerce/merchants	x	x	x	x
Acquirers/PSPs	x	x	x	x
Fintech	x	x	x	x
Technology				
On-premises	x	x	x	
Cloud-based	x	x	x	x
Hybrid	x	x		
Methodology				
Rule-Based	x	x		x
Machine Learning	x	x	x	x
Hybrid	x	x		
Data Ingestion				
Stateless Data ingestion and Augmentation	x			x
Machine Learning				
Supervised learning	x	x	x	x
Unsupervised learning	x		x	
Intelligence				x
Abuse List	x	x	x	x
Monitoring	x	x		
Address Verification	x	x		x
Credit Bureau	x	x		x
Information Sharing Network	x	x	x	
Case management	x	x	x	
Manual review	x	x		x
Orchestration layer	x	x		
Adaptive decisioning	x	x		
Chargeback management		x		
Recovery		x		
Guaranteed fraud prevention				

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	simility	ThreatMetrix	TrustStamp	Trulioo
IDENTITY VERIFICATION				
ID verification				
Identity Document Scanning	x	x	x	x
Video scanning			x	
Personally identifiable information (PII) Validation	x	x		x
Derived verification	x			
Small Transaction verification	x			
Email verification	x	x	x	x
Phone verification	x	x	x	x
Social verification	x		x	x
Additional checks/compliances				
Credit check	x	x		
Compliance check	x	x		x
AUTHENTICATION				
Behavioural biometrics		x		
Session analysis	x	x		
Device-user interaction	x	x		
Physical biometrics				
2-D facial recognition			x	x
Voice				
Fingerprint scan				
Iris scan				
Other				
Device fingerprinting	x	x	x	
Geo-location	x	x	x	
Remote access detection	x	x		
Mobile app push		x		
3-D secure 2.0	x	x		
Hardware token				
One-time passwords		x	x	
Knowledge-Based Authentication	x	x		

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company				
Customer Reference	Adaptive Decision-ing Platform Customers and Case Studies where applicable: US Bank, Zions Bank, OfferUp, Chime, Jumia, Luisaviaroma	Lloyds, risk-based authentication	More information upon request	Further details for case studies can be found here: https://www.trulioo.com/resources/case-studies/
Supported Regions	US Europe AsiaPac India China LATAM Africa Middle East	US Europe Middle East Africa AsiaPac India China LATAM ANZ	US UK Europe MENA APAC India China LATAM	Global

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	WEBSHIELD	wibmo
FRAUD DETECTION		
Target group		
Banks	x	x
Ecommerce/merchants	x	x
Acquirers/PSPs	x	x
Fintech	x	x
Technology		
On-premises		x
Cloud-based	x	x
Hybrid		x
Methodology		
Rule-Based	x	x
Machine Learning		x
Hybrid		x
Data Ingestion		
Stateless Data ingestion and Augmentation		x
Machine Learning		
Supervised learning		x
Unsupervised learning		
Intelligence		
Abuse List	x	x
Monitoring	x	x
Address Verification	x	
Credit Bureau	x	x
Information Sharing Network	x	x
Case management	x	x
Manual review	x	x
Orchestration layer		x
Adaptive decisioning		
Chargeback management		
Recovery		
Guaranteed fraud prevention		

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

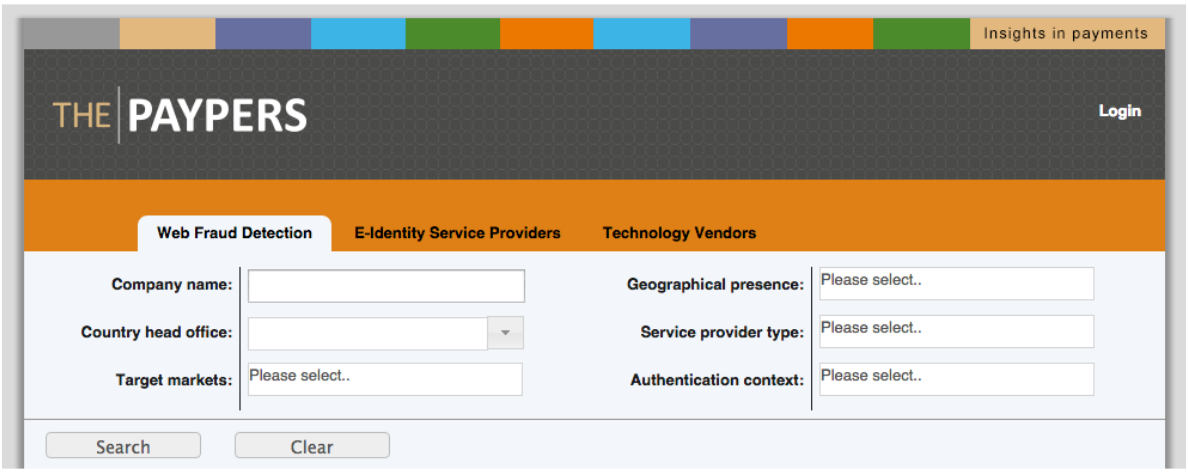
Company	WEBSHIELD	wibmo
IDENTITY VERIFICATION		
ID verification		
Identity Document Scanning	x	
Video scanning		
Personally identifiable information (PII) Validation	x	x
Derived verification		
Small Transaction verification	x	
Email verification	x	x
Phone verification	x	x
Social verification		
Additional checks/compliances		
Credit check	x	
Compliance check	x	x
AUTHENTICATION		
Behavioural biometrics		
Session analysis		x
Device-user interaction		x
Physical biometrics		
2-D facial recognition		
Voice		
Fingerprint scan		x
Iris scan		
Other		
Device fingerprinting		x
Geo-location		x
Remote access detection		
Mobile app push		x
3-D secure 2.0		x
Hardware token		
One-time passwords		x
Knowledge-Based Authentication		x

Fraud Detection, Identity Verification & Online Authentication – Mapping of Key Players

Company	WEBSHIELD	wibmo
Customer Reference	Wirecard Bank AG, Worldline SA, Concardis	More info upon request
Supported Regions	Global with emphasis on US Europe CIS	India APAC MENA Africa

THE PAYPERS

Visit Our Enhanced Online Company Profiles Database



All company profiles in the Web Fraud Prevention & Online Authentication Market Guide are available online in an enhanced company profiles database, complete with keywords, company logo and advanced search functionality.

https://webfraud-eidentity.thepaypers.com/

Company Profiles

Company	Fourstop GmbH (4Stop) View company profile in online database
4STOP	4Stop solves businesses' risk models through an all-in-one KYC, compliance, and anti-fraud solution. Their technology brings together proprietary real-time anti-fraud technology with thousands of global data points and hundreds of global KYC data sources, in a single integration. Resulting in an unrivalled combination to confidently anticipate risk and make quantifiable decisions to manage regulatory obligations and accelerate business performance.
Website	https://4stop.com
Keywords for online profile	fraud prevention, payment gateway, risk management, web fraud, detection, KYC, cybersecurity, regtech, digital identities, compliance, big data
Business model	Software-as-a-Service (SaaS)
Target market	Financial institutions, payment service providers, payment gateways, online communities/ web merchants, cryptocurrency, card issuers, gaming and gambling, money remittance providers, other online businesses
Contact	sales@4stop.com; info@4stop.com
Geographical presence	Global
Active since	2016
Service provider type	Digital identity service provider/web fraud detection company/technology vendor
Member of industry associations and or initiatives	FinTech Circle, RegTech Forums
Services	
Unique selling points	4Stop leverages its platform to enable merchants to screen for multiple fraud use cases including payment, loyalty, and social media reputation. Our unique capabilities allow customers to be efficiently removed from fraud processes, supporting merchant growth.
Core services	Card-not-present (online, IVR, call centre, and mobile) and card-present fraud prevention, fraud and risk consultancy, customer on boarding and payment transactional validation/ verification/authentication services.
Pricing Model	Pricing is per data source call/transaction and based on volume and complexity, and core services.
Fraud prevention partners	For more information please contact an account representative at sales@4stop.com or info@4stop.com
Other services	Account takeover, new account registration, payment fraud prevention, frictionless authentication and verification, bot detection, professional services, merchant onboarding
Third party connection	Aggregated APIs for KYC validation, verification, and authentication services
Technology: anti-fraud detection tools available	
Address verifications services	Yes
CNP transactions	Yes
Card Verification Value (CVV)	Yes
Bin lookup	Yes
Geo-location Checks	Yes
Device Fingerprint	Yes
Payer Authentication	Yes
Velocity Rules – Purchase Limit Rules	Yes
White list/black list database	Yes
KYC – Know Your Customer	Yes
Credit Rating	Yes
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities
Other	Profiling (dynamic summarisation and aggregation), account associations, data science, simulation reports, data market profiles

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call centre	No
other	For more information please contact an account representative at sales@4stop.com or info@4stop.com
Reference data connectivity	
Connectivity to governmental data	Yes
Other databases	4Stop references hundreds of databases from our partners, which include validation, verification, and authentication type providers leveraging from the following: - credit - government - commercial - consumer/social - utility - telco - postal - proprietary
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	No
Certification	
Type	ISO 27001, ISO 9001, TS 101 456, SAS70
Regulation	KYC, anti money laundering (AML), PSD2, MLD 4&5, GDPR
Other quality programmes	Ethical hacking, privacy compliance
Other remarks	For more information please contact an account representative at sales@4stop.com or info@4stop.com
Clients	
Main clients / references	Client Integrations of 4Stop: - Mifinity – https://4stop.com/media/mifinity-presser.html - Gatehub – https://4stop.com/media/gatehub-presser.html - PaySend – https://4stop.com/media/paysend-presser.html - Paymentz – https://4stop.com/media/paymentz-presser.html - Ontology – https://4stop.com/media/ontology-presser.html
Future developments	Upcoming product technology enhancements will include: enhancing the current platform and technology functionality with optimal user experience design, further technology developments in data analytic reporting output and monitoring capabilities, behaviour and machine learning, advanced account associations, and on-going KYC data source aggregation.

4STOP

Thousands Of Global Data Points.

Instantly access the worlds largest KYC / KYB data aggregation via one API, with real-time anti-fraud technology and intelligence for automated risk controls.

HUNDREDS OF KYC DATA SOURCES

Activate in real-time with cost-saving cascading logic.

AUTOMATED MERCHANT UNDERWRITING

Results in under 7 minutes with ability to KYC directors.

FUTURE-PROOF COMPLIANCE WORLD-WIDE

Stay abreast and manage on-going regulatory updates.

MULTI-FACETED AUTOMATED RISK ENGINE

Simple rule wizard, free-form scripting, endless rules.

REAL-TIME MONITORING & INTELLIGENCE

Through a single API enjoy a centralised view of risk.

DATA SCIENCE & GLOBAL DATA POINTS

Add to your KYC integrations in a frictionless manner.

All-In-One Global KYC, Compliance and Anti-Fraud Solution.

sales@4stop.com | www.4stop.com

Company	American Express Enterprise Fraud Management Solutions: Accertify & InAuth, Inc	View company profile in online database
	Accertify and InAuth are wholly-owned subsidiaries of American Express. Accertify is a leading provider of fraud prevention, chargeback management, and payment gateway solutions. InAuth is a leading digital device intelligence company for today's evolving digital world. Both companies help businesses reduce fraud, increase revenue, and enable frictionless experiences for good customers.	
Website	Accertify.com and InAuth.com	
Keywords for online profile	device identification, device intelligence, device reputation, risk detection, fraud prevention, chargeback management, fraud managed services, payment gateway	
Business model	Software-as-a-Service (SaaS)	
Target market	- online shoppers - ecommerce/mcommerce - financial institutions - payment services providers - government services - online communities/web merchants - gaming and gambling - ride sharing - travel and airlines - healthcare - other online businesses	
Contact	Michael.Lynch@InAuth.com	
Geographical presence	North America, LATAM, JAPA, APAC, EMEA	
Active since	2008	
Service provider type	- digital identity service provider - technology vendor - enterprise web fraud detection company	
Member of industry associations and or initiatives	MRC, FIDO, AICPA (SOC), IATA, MAG, Airline Information Organization, and more	
Services		
Unique selling points	When a customer accesses your mobile app or website, InAuth leverages hundreds of device attributes to uniquely identify it. InAuth also assesses high-risk indicators that could indicate a fraud attempt. We help you to know and understand the trustworthiness of every device interacting within your digital channels. The Accertify fraud management solutions put you in control to identify and prevent account takeovers, account originations schemes, and payment fraud.	
Core services	Browser and app based device intelligence and risk detection	
Pricing Model	Transaction based pricing	
Fraud prevention partners	Actimize, AimBrain, Early Warning, Everis, Emailage, Whitepages Pro, and more	
Other services	Secure communcation, PSD2 compliance, account takeover, new account opening, payment fraud prevention, frictionless authentication, bot detection, professional services	
Third party connection	For more information please contact Accertify or InAuth	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	Yes	

Velocity Rules – Purchase Limit Rules	Yes
White list/black list database	Yes
KYC – Know Your Customer	Yes
Credit Rating	Yes
Follow up action	Out of band push notification
Other	Bot detection, malware detecton, fraud tool detection, location spoofing detection, JailBreak/root detection, malicious application detection
Authentication Context	
Online	Yes
Mobile	Yes
ATM	Yes
POS	No
Call centre	Yes
other	N/A
Reference data connectivity	
Connectivity to governmental data	No
Other databases	No
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	Soc2, GDPR, PCI
Regulation	For more information please contact InAuth or Accertify
Other quality programmes	Penetration testing, privacy compliance
Other remarks	For more information please contact Accertify or InAuth
Clients	
Main clients / references	Not disclosed – Contact us for more information
Future developments	Not disclosed – Contact us for more information

Accertify
AN AMERICAN EXPRESS COMPANY
10 YEARS

InAuth

American Express Enterprise Fraud Prevention Solutions

Accertify.com

InAuth.com

Heightened security on the digital channels with next generation fraud management solutions

- Fraud Prevention
- Frictionless Authentication
- Mobile & Browser Security

Banking | Payments | Commerce | Travel | Enterprise

Company	Arvato Financial Solutions	View company profile in online database
arvato BERTELSMANN	Arvato Financial Solutions provides professional financial services to renowned international brands as well as respected local businesses – allowing them to leave their credit management to a professional, so they can focus on what matters most for their business. Our services center around cash flow in all segments of the customer lifecycle: from identity, fraud and credit risk management, to payment and financing services and debt collection.	
Website	www.finance.arvato.com	
Keywords for online profile	fraud management, fraud prevention, behavioural biometrics, ecommerce, mobile banking	
Business model	Software-as-a-Service (SaaS), managed services, consulting services, support services, and decision science	
Target market	Ecommerce, finance and payment, telco, IT, media and entertainment	
Contact	Dario Artico (dario.artico@arvato.com)	
Geographical presence	North America, Latin America, Europe	
Active since	1960	
Service provider type	Identity, fraud and credit risk management, payment, financing and debt collection services	
Member of industry associations and or initiatives	Merchant Risk Council (MRC)	
Services		
Unique selling points	The Arvato Financial Solutions team is made up of proven and reliable experts in around 20 countries, including 7,500 IT, analytics, process and legal specialists, dedicated to revealing the advantages of big data, advanced foresight, predictive analytics and strategic consultancy. All employees share one common goal: to make client's credit management run effortlessly and effectively, enabling optimised financial performance. Arvato Financial Solutions can give businesses the best possible platform for growth.	
Core services	Identity and fraud management, credit risk management, payment and financing services, debt collection services	
Pricing Model	Contact us for current pricing information	
Fraud prevention partners	SecuredTouch, Inform	
Other services	Information available upon request	
Third party connection	Information available upon request	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	Yes	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	Yes	
Follow up action	Manual Order Review	
Other	Information available upon request	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	Yes
Call centre	Yes
other	Information available upon request
Reference data connectivity	
Connectivity to governmental data	No
Other databases	Yes
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	ISO 27000, ISAE 3402, DataCenter ISO 9001
Regulation	GDPR, Payment Institution License
Other quality programmes	Information available upon request
Other remarks	ISO27001 foundation, int. Auditor ISO27001, Cobit 5 foundation, ITIL V3 (Op/ST/SD/CSI), Prince2, IT Security Manager (CCI), Technical IT Security specialist (CCI), Quality Management Officer (German Accreditation Body), Data Protection Officer (CCI), SAP Foundation, MCP, MCSA, MSCE
Clients	
Main clients / references	We work with: - three of the top five global internet companies - four of the top 10 global telcos - the six big UK utility providers - all German insurance providers. We work for global renowned brands, as well as for local respected businesses.
Future developments	Contact us for further information

Enabling growth – through seamless and secure financial transactions

Let's face it: fraud is an increasing challenge.

By means of advanced foresight, predictive analytics and strategic consultancy, we efficiently guide you through complexity. We replace uncertainty and risk with structure and trust, so you can focus on what matters most for your business.

Give your company the best possible platform for growth with Arvato Financial Solutions. We provide services in all segments of the customer lifecycle: from identity, fraud and credit risk management, to payment, financing and debt collection.

Your advantages:

- Reduced fraud losses
- Increased conversion rate
- Optimised processes and workflows
- Brand protection

What we do, so you can focus on your core business:

STOPPING FRAUD BEFORE IT HAPPENS THROUGH EARLY PREVENTION

IDENTIFYING GOOD USERS AND IMPROVING THEIR CUSTOMER EXPERIENCE

DETECTING ANOMALIES AND FRAUD PATTERNS INTELLIGENTLY

Financial Solutions

Do you have further questions? Please feel free to contact us.
Arvato Financial Solutions – Your backbone for growth.

www.finance.arvato.com

arvato
BERTELSMANN

Company	BioCatch	View company profile in online database
	BioCatch is a digital identity company that delivers behavioural biometrics, analysing human-device interactions to protect users and data. Banks, financial institutions and other enterprises use BioCatch to significantly reduce online fraud and friction costs, and protect against a variety of cyber threats, without compromising the user experience.	
Website	www.biocatch.com	
Keywords for online profile	behavioural biometrics, identity proofing, continuous authentication, fraud prevention	
Business model	BioCatch leverages behavioural biometrics to track user interactions and responses within web and mobile applications. This provides banks, ecommerce companies and other enterprises with a strong value proposition: we can detect the most advanced fraud attacks and cyber threats with an amazing degree of accuracy. We provide business value in two primary areas: - Less Friction: Currently, a high percentage of genuine users fail step-up authentication in online banking leading to low customer satisfaction and higher call-center/ fraud-management operational costs. BioCatch Behavioural Biometrics authenticates over a very high percentage of genuine sessions thus reducing the number of failed authentication attempts and associated operational call center costs. - Less Fraud: Existing security solutions are becoming less effective in distinguishing between genuine users and fraudsters. BioCatch is able to prevent various types of fraud such as social engineering schemes and non-human attacks by bots, aggregators, malware and remote access Trojans.	
Target market	BioCatch is currently targeting the following vertical markets: banking, ecommerce, financial services (e.g. credit bureaus and unions), credit card issuers, insurance, payroll systems, and mobile device manufacturers.	
Contact	Kevin Donovan, VP of Sales, Americas, kevin.donovan@biocatch.com; Richard Perry, VP of Sales, EMEA, richard.perry@biocatch.com; Oren Kedem, VP of Sales, LATAM	
Geographical presence	BioCatch has a strong global presence in all geographic territories. In particular, the US, EMEA and LATAM.	
Active since	2011	
Service provider type	BioCatch is a technology vendor that fits two of your categories: Web Fraud Detection Company. One of our core capabilities is fraud prevention. BioCatch is capable of identifying sophisticated forms of account takeover through behavioural profiling and threat detection without impacting the user experience. This is used to either escalate a session or activity that receives a high score, or alternatively to de-escalate the activity even if other security or fraud controls suggest it is risky, allowing the customer to reduce friction and operational costs. BioCatch excels in providing a near-Zero-FP detection of a variety of advanced attacks: bots, MITB attack, social engineering and RATs (Remote Access).	
Member of industry associations and or initiatives	Biometrics Institute.	
Services		
Unique selling points	- Technology: BioCatch's unparalleled patent portfolio drives extremely high accuracy with minimal false alarms. - Experience: BioCatch's solution is widely deployed by leading banks and financial institutions around the world; - Expertise: BioCatch is spearheaded by a strong "bench" of experts from various scientific disciplines.	
Core services	BioCatch behavioural biometrics has three primary capabilities that provide great value to customers: Identity Proofing, Continuous Authentication (through passive behavioural profiling) and Fraud Prevention. In regards of fraud prevention, BioCatch is able to effectively combat a variety of threats, such as: malware, bots/aggregators, remote access Trojans and social engineering.	
Pricing Model	BioCatch's pricing model is based on an annual license and a one-time setup fee on a per user or transaction basis.	
Fraud prevention partners	BioCatch has partnerships with: Microsoft, LexisNexis, Nuance, Experian, Samsung SDS and Forgerock.	

Other services	For Identity Proofing BioCatch behavioural biometrics offers a new dimension to fighting new account fraud. The system distinguishes between a real user and an impostor by recognizing normal user behaviour and fraudster behaviours, even when no profile exists. Understanding how criminals behave online, the BioCatch Identity Proofing Module looks at 3 elements to generate a risk score: Application Fluency: most fraudsters use compromised or synthetic identities to repeatedly attack a site. These actions show a fluency with the site and the process used to open a new account. Navigational Fluency: fraudsters often use advanced computer skills that are rarely seen among real users. Common examples include keyboard shortcuts and function keys. Low Data Familiarity: fraudsters exhibit several behavioural traits when they enter in unfamiliar data.
Third party connection	BioCatch has numerous business partnerships with a wide variety of industry players. Two prominent examples: Experian - a leading a consumer credit reporting agency that collects and aggregates information on over one billion people and businesses and Lexis Nexis - providing computer-assisted legal research as well as business research and risk management services. BioCatch has a very strong and ever-growing partnership with Microsoft - BioCatch technical operations are supprted by Microsoft Azure.
Technology: anti-fraud detection tools available	
Address verifications services	N/A
CNP transactions	N/A
Card Verification Value (CVV)	N/A
Bin lookup	N/A
Geo-location Checks	BioCatch's geo-location checks capability is based on collecting a large number of network and device-related parameters for PCs and Mobile devices, such as: IP, IP ASN, IP ISP, IP City, IP Country, Time Zone and additional factors. All of these are amalgamated to a strong geo-location check. Of course, this is optional – based on the customer's needs and use case.
Device Fingerprint	BioCatch generates several device prints with different accuracy levels. Those are used internally to support the device recognition capability. An example of those device prints is below: - Most unique – 1:109 – this is typically used to ensure device is not spoofed, but is very sensitive to changes in the device configuration. However if we see this value again, it means it has to be the regular user device. - Medium uniqueness – 1:2,000,000 – this is the "standard" device recognition resolution. - Fuzzy Uniqueness – 1:10,000 – this may confuse two similar devices as one, but on the other hand it leverages network information to highly correlate/associate those devices with the user (e.g. same Wifi being used), so chances of the second device to be used for fraud is very slim.
Payer Authentication	With Behavioural Biometric Profiling, customers can call on BioCatch at any point during the session to ascertain the identity of the user (i.e. verifying users with low scores) or detect very-high-risk account takeover cases in real time (i.e. feeding our high risk scores into their risk management system). The deliverable is a 0-1000 score, where the score range is calibrated to the desired alert rate (e.g. 900+ is 0.25% alert rate). Through this advanced capability, BioCatch is able to continuously authenticate payers during online sessions.
Velocity Rules – Purchase Limit Rules	N/A

White list/black list database	The BioCatch system learns not just from the good guys, but also from the bad guys. Using a robust white/black list database, we train the system for generic criminal patterns. Here the focus is not on profiling users, but rather on seeing how criminals behave when doing fraud. The system takes into account behavioural and cognitive analysis, plus additional information such as device, network, context of the transaction and other factors. The result is then integrated together with the behavioural profiling score into a single integrated score. This way we can provide a score for every session, even if the user does not yet have a mature profile. The system also takes into account individual fraudster behaviour by consulting with a common repository of known frauds. Not every individual fraudster can be profiled, but in many cases a specific cybercriminal will have unique traits – the equivalent of a nasty scar or a recognisable tattoo that makes them easy to spot in a police lineup.
KYC – Know Your Customer	BioCatch supports KYC operations through its identity proofing capability, using application fluency, navigational fluency and data familiarity. Traditional KYC profiling validates the information provided by the user, compared to a reliable source (e.g. DMV database). However, recent data breaches have exposed this data publicly. BioCatch's identity proofing capability is able to distinguish between the genuine user providing data and a fraudster providing the exact same data, through behavioural profiling.
Credit Rating	N/A
Follow up action	BioCatch's technology is built to support risk-based authentication, by feeding profiling scores into ther platform rules engines. The platforms usually specify the follow-up actions on a case by case basis.
Other	Invisible Challenges are patented techniques that introduce subtle tests into the online session that users subconsciously respond to without sensing any change in their experience. The response contains behavioural data that is used to distinguish a real user from an imposter, whether human or non-human (robotic activity, malware, aggregator, etc.). It is important to note that BioCatch's team of researchers test each challenge and its corresponding deviation to determine the threshold at which users notice a change in experience on the mobile or website. Example: Disappearing Mouse/Challenge: Hide the cursor. Users search for the cursor/mouse in very different and unique ways. Some use wide search patterns, others use small ones, some are horizontal while others are diagonal, and certain users always search counter-clockwise. Sometimes users move on a certain learning curve and their responses vary according to their location on the curve. All these can be captured as unique parameters, however, typically this is not practical, because the time required for the user to provide enough relevant mouse movements to accurately authenticate themselves is too long. Invisible Challenges unconsciously "forces" the user to make various mouse movements in a very short time, allowing BioCatch to capture adequate data from the user in 500 milliseconds, making it useful for detecting anomalies in user behaviour in near real-time.
Authentication Context	
Online	Yes: We support JavaScript integrations with the following browsers: Internet Explorer, Chrome, Firefox.
Mobile	Yes: We support SDK integrations with iOS and Android.
ATM	N/A
POS	N/A
Call centre	N/A
other	N/A
Reference data connectivity	
Connectivity to governmental data	N/A
Other databases	N/A

Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Cross-Channel Fraud: Many of our customers use BioCatch to detect fraud that begins or ends in the online channel, but then carried out at a different channel. For example – a customer in Spain is using the system to detect whether a fraudster illegally accesses the user online banking account, then goes to the credit cards balance section to copy the user's credit card number and expiration date – this can be later used for ecommerce fraud. The combination of an abnormal behaviour with a risky context (copying information in the cards balance page) is highly accurate – no false positives. BioCatch has partnerships with other leading industry vendors that provide complimentary biometric authentication solution. In this regard, BioCatch's partnership with Nuance Communications stands out, as behavioural biometric risk scores are fed into their call center's fraud systems. This has been very effective in combating cross-channel fraud.
Certification	
Type	SOC 2 Type II: BioCatch complies with highest security standards when it comes to security. BioCatch is SOC2 Type II[1] (Security and Availability) certified since February 15th 2015 by E&Y. Annual SOC2 reviews are conducted to maintain and comply with highest industry standards. The audit/report can be provided upon demand
Regulation	BioCatch complies with GDPR, PSD2 and Open Banking initiatives.
Other quality programmes	
Other remarks	
Clients	
Main clients / references	BioCatch is implemented in global tier-1 financial institutions, with more than 5 billion transaction per month covering more than 50 million users. Detailed Case studies here. https://www.biocatch.com/resources/case-studies/a-top-5-u.s.-bank-detects-trickbot-malware-attacks-with-biocatchs-behavioral-biometrics-solution Individual reference details for each bank available on request.
Future developments	In 2018, BioCatch is planning on massive expansion of use cases as the capability of behavioural biometrics extends beyond the traditional fraud prevention realm into on-device authentication and new fraud areas; new verticals, to go beyond banking and expanded partnerhips.

Company	CA Technologies	View company profile in online database
	CA Technologies, a Broadcom company, is an industry leader in payment and identity fraud prevention, with friction-free transaction authentication powered by patented artificial intelligence. As a pioneer in data analytics for online fraud, CA delivers a unique 360-degree view of transactions for issuers, processors, and merchants, across all payment schemes. Learn more at **ca.com/balance.**	
Website	www.ca.com	
Keywords for online profile	authentication, 3-D Secure 2.0, EMV 3-D Secure, fraud prevention, predictive analytics	
Business model	SaaS	
Target market (limited list of markets)	- financial institutions/card issuers - acquirers/processors - ecommerce merchants	
Contact	paymentsecurity@ca.com	
Geographical presence	Global	
Active since	1997 (initially as Arcot Systems, acquired by CA Technologies in October of 2010)	
Service provider type	Technology vendor, card-not-present fraud prevention solutions, 3DS 2.0 provider, EMV 3-D Secure, strong authentication and risk analytics, identity fraud prevention	
Member of industry associations and initiatives	Merchant Risk Council, US Payments Forum, EMVCo Technical Associate	
Services		
Core services	PSD2 compliance, Authentication, 3-D Secure, predictive analytics, risk analytics network, fraud detection	
Other services	For more information contact our Sales Director, Graeme.Bullock@ca.com	
Unique selling points	As a pioneer in 3-D Secure and a leader in risk analytics for online fraud—powered by the largest risk analytics network in the industry—CA Technologies delivers a unique 360° view of card-not-present transactions that offers real-time authentication for issuers, processors and merchants, across all payment schemes. Its patented neural network technology protects everything from ecommerce and online banking to authentication for enterprise systems.	
Pricing	Transaction-based pricing, price bands for number of transactions processed.	
Partners	TSYS, First Data, FIS, PSCU	
Offering: authentication technology used		
PIN	Yes	
Password/phrase	Yes	
Token	Yes: cryptographically protected soft tokens	
Card	N/A	
Digital certificates (hosted yes/no)	Yes	
Multifactor authentication	Yes	
Biometrics:	Yes	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	N/A	
Branch/Point of Sale	N/A	
Call Centre	Yes	
Other	ecommerce payments, online banking and similar enterprise use cases	

Reference data connectivity	
Connectivity to governmental data	For more information contact our Sales Director, Graeme.Bullock@ca.com
Other databases	CA Risk Analytics Network: CA has anonymized data (device ID, geolocation, merchant transaction type, and more) within its risk analytics customer network. CA Neural Network models and machine learning techniques use this data to produce a more accurate risk score to help determine whether a transaction is legitimate or fraudulent. CA Technologies leverages Neustar geo-location intelligence.
Certification	
Type	SSAE 18 SOC 1, Type 2, SSAE 18 SOC 2, Type 2, Visa ACS, PCI-DSS
Regulation	Solution allows customers to comply with the PSD2 SCA regulation
Other quality programs	PCI-DSS compliant
Other remarks	For more information contact our Sales Director, Graeme.Bullock@ca.com
Clients	
Main clients / references	For more information contact our Sales Director, Graeme.Bullock@ca.com
Future developments	For more information contact our Sales Director, Graeme.Bullock@ca.com

Striking a Balance

Enhance fraud protection while enabling a frictionless customer experience.

For nearly 20 years, CA Technologies has led the way in authentication and fraud prevention, providing a unique 360° view of card-not-present transactions. As the world's largest 3-D Secure (3DS) provider, we were first to deploy 3DS and the first to authenticate an EMV® 3DS transaction—delivering state-of-the-art protection and a seamless customer experience. Our patented fraud analytics give issuers, processors, and merchants the real-time insights they need to reduce false declines and increase conversions—all with the strong authentication required to achieve PSD2 compliance.

To learn more, visit us at **ca.com/balance**

ca technologies
A Broadcom Company

Industry-Leading Authentication Solutions

CA Payment Security Suite • CA Risk Analytics Network • CA Identity Risk Insight Suite

Company	CashShield	View company profile in online database
	CashShield is a global online fraud management company that helps enterprises manage their risk from fraudulent payments and accounts. Uniquely powered by high-frequency trading algorithms combined with real-time pattern recognition and passive behavioural biometrics, CashShield's award-winning solution functions without the need for any data scientists or fraud analysts.	
Website	www.cashshield.com	
Keywords for online profile	fraud solution, account takeover, authentication, real-time, instant decisions, chargeback guarantee	
Business model	SaaS fraud management solution	
Target market	Financial institutions, government services, online communities/web merchants, gaming and gambling, other online businesses	
Contact	enquiries@cashshield.com / +65 6569 3686	
Geographical presence	Global (offices in San Francisco, Shanghai, Berlin, Singapore, Jakarta)	
Active since	2008	
Service provider type	Web fraud detection company	
Member of industry associations and or initiatives	For more information, please contact the company	
Services		
Unique selling points	CashShield is the world's first and only full-machine automated solution that functions without the need for any human involvement. CashShield's real-time solution provides instant decisions to accept or reject transactions, logins and/or account creations, ensuring maximum scalability especially during promotional periods, with 100% chargeback protection for physical and digital goods.	
Core services	Fraud risk management for online transactions and accounts	
Pricing Model	% fee of value of transactions	
Fraud prevention partners	N/A – all of CashShield's technology is built in-house	
Other services	Fraud analytics	
Third party connection	N/A	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	Yes	
Velocity Rules – Purchase Limit Rules	No: CashShield does not use hard rules or limits that hampers growth	
White list/black list database	Yes	
KYC – Know Your Customer	No	
Credit Rating	No	
Follow up action	Our fully managed service provides real-time decisions: accept or reject. We make decisions, not predictions.	
Other	CashShield's end-to-end solution provides comprehensive protection at various points of entries and vulnerabilities, including credit transfer, withdrawals, account creations and account logins.	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	Yes
Call centre	Yes
other	For more information, please contact the company
Reference data connectivity	
Connectivity to governmental data	No
Other databases	Yes
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCI DSS Level 1
Regulation	For more information, please contact the company
Other quality programmes	For more information, please contact the company
Other remarks	For more information, please contact the company
Clients	
Main clients / references	Alibaba, Razer, Grab, Yamibuy, Creative Group, Garena (SEA), Scalefast, Voyagin
Future developments	Adding on a suite of solutions to complete our comprehensive end-to-end fraud protection tailored for enterprises

CASHSHIELD

Make Decisions, Not Predictions

The world's first fraud detection solution with real-time decisioning without the need for human involvement

1. CHECK OUT/ LOGIN

User logs in or checks out to make payment with no unnecessary additional verification.

2. REAL-TIME ANALYSIS

CashShield fraud engine analyzes customer behavior in real-time to filter away fraudulent activity.

3. OPTIMIZED DECISION

Uniquely incorporated high frequency algorithms returns optimized decisions instantly: **accept** or **reject**.

Learn how to unlock your maximum potential at
www.cashshield.com

Singapore | San Francisco | Shanghai | Berlin | Jakarta

Company	Computop	View company profile in online database
	Computop offers local and innovative omnichannel solutions for payment processing and fraud prevention around the world. For ecommerce, at POS, and on mobile devices, retailers and service providers can choose from over 250 payment methods. Computop, a global player with locations in DE, CN, the UK, the US, processes transactions for more than 15,000 retailers annually, with a combined value of USD 31 bln.	
Website	www.computop.com	
Keywords for online profile	payment, fraud, machine learning, credit card, 3-D Secure, conversion, PSP, payment processing, ecommerce	
Business model	Payment service provider	
Target market	- online and stationary retail - financial institutions - payment service providers - online communities/web merchants - gaming and gambling	
Contact	Germany: +49 (951) 98009-22, sales@computop.com UK: +44 (0) 1932 895735, uk@computop.com USA: +1 800 701 7806, usa@computop.com China: +86-152 1432 8818, info@computop-china.cn	
Geographical presence	North/Latin America, Europe, Middle East/Africa, Asia/Pacific	
Active since	1997	
Service provider type	Payment service provider (PSP)	
Member of industry associations and or initiatives	Please contact Computop for more information	
Services		
Unique selling points	Global omnichannel payment, international card processing and local payment processing, P2PE-certified POS-terminal solutions, mobile SDK for In-App payments, receivables management, currency conversion, individual payment forms for all channels, efficient and customisable fraud prevention with machine learning algorithms, intelligent 3-D Secure handling, biometric authentication, reduced integration effort through pre-integration with leading ERP, and ecommerce vendors including: Salesforce CC, hybris, IBM WebSphere, INTERSHOP, Magento, Oxid eSales, Spryker, SAP, and more, independent industry and product consultancy	
Core services	Complete omnichannel solution for global payment processing (ecommerce, mcommerce, POS, MOTO) as well as “out of the box” mobile templates; extensive risk management and fraud protection	
Pricing Model	Provided upon request. Contact Computop for more information.	
Fraud prevention partners	Computop is connected to arvato infoscore, CEG, creditreform, Crif, Neustar and Schufa to run address and credit check on customers – whether individuals or companies – in several European countries. Further partners are Riskident, ACI ReD, Cardinal Commerce, and more.	
Other services	FIDO Server for biometric authentication in payments and beyond	
Third party connection	Please contact Computop for more information	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	Yes	

Velocity Rules – Purchase Limit Rules	Yes
White list/black list database	Yes
KYC – Know Your Customer	Yes
Credit Rating	Yes
Follow up action	Yes
Other	Please contact Computop for more information
Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	Yes
Call centre	Yes
other	Please contact Computop for more information
Reference data connectivity	
Connectivity to governmental data	No
Other databases	Schufa, CRIF, arvato infoscore, Neustar
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCI DSS Level 1, PCI P2PE
Regulation	Please contact Computop for more information
Other quality programmes	Please contact Computop for more information
Other remarks	Please contact Computop for more information
Clients	
Main clients / references	OTTO group, Sixt, Wargaming, Fossil, illy, Svarowski, CEWE, Rakuten, badoo, TUI
Future developments	Please contact Computop for more information

SMART AGAINST FRAUD

Rule Based becomes Risk Based:
Boost your conversion rate!

computop
the payment people

computop.com

Company	Covery	View company profile in online database
	Covery is a global risk management platform helping online companies solve fraud and minimise risk. We focus on the universality of our product and its adaptation to any type of business, based on the individual characteristics and customer needs using both rule-based and machine learning approaches.	
Website	covery.ai	
Keywords for online profile	machine learning, fraud prevention, trustchain, customization, risk management, online fraud, data processing	
Business model	SaaS	
Target market (limited list of markets)	Ecommerce, marketplaces, dating, gambling	
Contact	sales@covery.ai	
Geographical presence	EU	
Active since	2016	
Service provider type	Risk management, web fraud detection company, tech vendor	
Member of industry associations and initiatives	MRC	
Services		
Unique selling points	What we offer: - client data acceptance - rule-based machine learning - deep customization - free trial - compatible pricing - functionality to work with loyal users to increase revenue	
Core services	Risk management, fraud prevention	
Pricing	Pricing is per action, and based on volume and complexity.	
Partners	Maxpay	
Other services	For more information please contact the company	
Offering: authentication technology used		
PIN	N/A	
Password/phrase	N/A	
Token	N/A	
Card	N/A	
Digital certificates (hosted yes/no)	N/A	
Multifactor authentication	N/A	
Biometrics	N/A	
Authentication context		
Online	N/A	
Mobile	N/A	
ATM	N/A	
Branch/Point of Sale	N/A	
Call Centre	N/A	
Other	N/A	
Reference data connectivity		
Connectivity to governmental data	Yes	
Other databases	Yes	

Certification	
Type	N/A
Regulation	N/A
Other quality programs	N/A
Other remarks	N/A
Clients	
Main clients / references	N/A
Future developments	Automated ML helper for risk logic tuning

COVERY
SOLVE FRAUD

POWER UP YOUR RISK TEAM

And maximize revenue with more adaptive fraud analysis

Covery's rule-based and machine learning approach adapts to each business' individual characteristics and needs, no matter whether you are in the high-risk or low-risk industries.

This is only a part of the benefits your Risk Team receives:

- Wider coverage of your customer actions for analysis
- Flexible and rapid customization of data patterns
- Usage of any your in-house data for analysis
- Rule-based and machine learning approaches
- Tools to work with your loyal customers
- Simple integration with your business processes
- Creation of custom machine learning models
- New individual functionality for your business

COVERY. POWER UP YOUR RISK TEAM. SOLVE FRAUD

Company	CyberSource Ltd. View company profile in online database
CyberSource® A Visa Solution	CyberSource is a global, modular payment management platform built on secure Visa infrastructure with the benefits and insights of a vast USD 427 billion global processing network. This solution helps businesses operate with agility and reach their digital commerce goals by enhancing customer experience, growing revenues, and mitigating risk. For acquirer partners, CyberSource provides a technology platform, payments expertise, and support services that help them grow and manage their merchant portfolio to fulfill their brand promise. For more information, please visit cybersource.com.
Website	www.cybersource.com
Keywords for online profile	fraud management, risk management, payment security, ecommerce, payments, payment gateway, account takeover, rules based payer authentication, loyalty fraud
Business model	Software-as-a-Service (SaaS)
Target market	Retail, gaming, FX, financial services, travel, airline, transit, hospitality, insurance, utilities, telco services, government, digital content, internet service providers, media
Contact	www.cybersource.com/contact_us
Geographical presence	Global
Active since	1994
Service provider type	Payment Service Provider (PSP), fraud management, web fraud detection, device identification, acquirer partner network, payment management company, payment gateway, processor
Member of industry associations and or initiatives	Merchant Risk Council, IMRG, Vendorcom
Services	
Unique selling points	CyberSource is a global, modular payment management platform built on secure Visa infrastructure with the benefits and insights of a vast USD 427 billion global processing network. This solution helps businesses operate with agility and reach their digital commerce goals by enhancing customer experience, growing revenues, and mitigating risk.
Core services	CyberSource offers a multi-layered fraud management solution – from account monitoring to transaction fraud detection, rules tuning to payer authentication – that helps businesses minimise fraud losses, maximise revenue, and minimise operational costs.
Pricing Model	Tiered SaaS-based pricing model
Fraud prevention partners	ThreatMetrix, Cardinal Commerce, Neustar
Other services	More information available upon request
Third party connection	Neustar, LexisNexis, Whitepages.com, Perseuss, Computer Services, Emailage
Technology: anti-fraud detection tools available	
Address verifications services	Yes
CNP transactions	Yes
Card Verification Value (CVV)	Yes
Bin lookup	Yes
Geo-location Checks	Yes
Device Fingerprint	Yes
Payer Authentication	Yes
Velocity Rules – Purchase Limit Rules	Yes
White list/black list database	Yes
KYC – Know Your Customer	No
Credit Rating	No
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities
Other	More information available upon request

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call centre	Yes
other	More information available upon request
Reference data connectivity	
Connectivity to governmental data	No
Other databases	Commercial attribute providers, e.g. credit databases
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	More information available upon request
Regulation	More information available upon request
Other quality programmes	More information available upon request
Other remarks	Contact europe@cybersource.com for more information.
Clients	
Main clients / references	GAME, GHD, Aeromexico, Turkish Airlines, Cinépolis, Webjet, Backcountry, ESET
Future developments	For more information contact europe@cybersource.com.

CyberSource®
A Visa Solution

Powered by machine learning. Controlled by you.

Win epic battles against fraud using smart machine learning, combined with flexible rules. CyberSource Decision Manager combines machine learning with rules that let you precisely control your online fraud management strategy.

Half human, half machine – the best of both worlds.

cybersource.co.uk/machinelearning

Company	DataVisor	View company profile in online database
	DataVisor is a cutting edge fraud detection platform based on machine learning. Using proprietary unsupervised machine learning algorithms, DataVisor helps restore trust in digital commerce by helping businesses proactively detect and prevent fraud. Combining advanced analytics and an intelligence network of more than 4B user accounts globally, DataVisor protects businesses against financial and reputational damage.	
Website	datavisor.com	
Keywords for online profile	machine learning, fraud, unsupervised machine learning, unknown fraud, account takeover fraud, transaction fraud, financial crime, application fraud	
Business model	SaaS	
Target market (limited list of markets)	- online shoppers - financial institutions - payment service providers - government services - online communities/web merchants - gaming and gambling - other online businesses	
Contact	Priya Rajan	
Geographical presence	US, EMEA and APAC	
Active since	2014	
Service provider type	Technology vendor (other types can be added, if applicable)	
Member of industry associations and initiatives	For more information please contact the company	
Services		
Core services	Technology solutions for detecting fraud	
Other services	Transaction services (offering connectivity to other credential issuers)	
Unique selling points	DataVisor uses proprietary unsupervised machine learning algorithms to provide early detection of emerging fraud patterns without the need of historical loss labels or lengthy training periods. Since its predictive power is not based on historic labels, DataVisor can provide early detection with high accuracy even without frequent model re-tuning.	
Pricing	For more information please contact the company	
Partners	Microsoft, AWS	
Offering: authentication technology used		
PIN	For more information please contact the company	
Password/phrase	For more information please contact the company	
Token	For more information please contact the company	
Card	For more information please contact the company	
Digital certificates (hosted yes/no)	For more information please contact the company	
Multifactor authentication	For more information please contact the company	
Biometrics:	Face recognition, palm/fingerprint recognition	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	For more information please contact the company	
Branch/Point of Sale	For more information please contact the company	
Call Centre	For more information please contact the company	
Other	For more information please contact the company	

Reference data connectivity	
Connectivity to governmental data	Citizens register, company register, IDs
Other databases	Commercial attribute providers, credit databases
Certification	
Type	ISO 27001, ISO 9001, TS 101 456, SAS70
Regulation	KYC
Other quality programs	Ethical hacking, privacy compliance
Other remarks	For more information please contact the company
Clients	
Main clients / references	For more information please contact the company
Future developments	For more information please contact the company

DATAVISOR

DISCOVER THE UNKNOWN

Unsupervised Machine Learning for Fraud Prevention

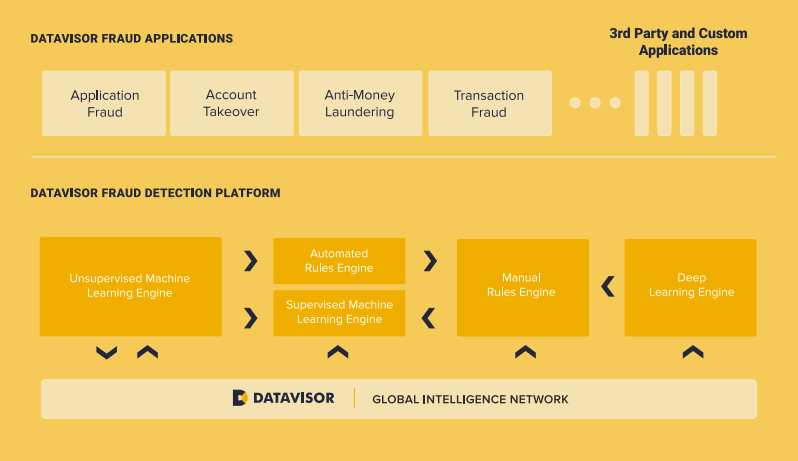
› No Historic Labels › No Lengthy Training Periods › No Frequent Retuning

AI-Based Fraud Detection for the Digital Era

- › APPLICATION FRAUD
- › ACCOUNT TAKEOVERS
- › ANTI-MONEY LAUNDERING
- › TRANSACTION FRAUD

DataVisor Enterprise

Comprehensive AI Fraud Detection Platform



www.datavisor.com

Company	Emailage	View company profile in online database
	Emailage, founded in 2012 and with offices across the globe, is a leader in helping companies significantly reduce online fraud. Through key partnerships, proprietary data, and machine learning technology, Emailage builds a multi-dimensional profile associated with a customer's email address and renders a predictive risk score. Customers realise significant savings from identifying and stopping fraudulent transactions.	
Website	www.emailage.com	
Keywords for online profile	online fraud prevention, email risk assessment, email address fraud prevention, CNP fraud prevention, global fraud prevention, transaction risk analysis, predictive fraud risk scoring, global consortium database	
Business model	For more information contact the company	
Target market	Ecommerce merchants, payment processors, financial institutions, airlines, OTA, ticketing brokers, money transfer companies, credit card issuers, marketplace lenders, personal computer manufacturers, fraud platforms, gaming and gambling, other online businesses	
Contact	Contact@emailage.com	
Geographical presence	Global	
Active since	2012	
Service provider type	Online fraud prevention and digital identity intelligence provider	
Member of industry associations and or initiatives	Merchant Risk Council, NORA Network (Australia)	
Services		
Unique selling points	Since 2012, Emailage has offered fraud risk assessment built around the email address. The company utilises a predictive risk score based on machine learning algorithms combined with a cross-industry and cross-sector consortium database. This approach offers merchants the ability to mitigate fraud with negative signals, while using positive signals to approve good customers.	
Core services	Email address + global network + machine learning algorithms = online predictive fraud risk score. We provide a secure, frictionless layer of protection that will supercharge your risk engine. Our predictive online fraud risk scoring uses email address metadata as the core for transactional risk assessment and identity validation. Our online identity profiles fuse this data with other elements, such as phone number, address, and customer name. Emailage helps reduce fraud for hundreds of customers around the world, including 5 of the top 10 global retailers, 3 of the top 5 largest global airlines, the top 3 PC manufacturers, 3 of top 6 credit card issuers, 3 of the top 5 marketplace lenders, the top 4 money transfer providers, and 3 of the top 5 travel websites. This year to date, Emailage has analysed nearly USD 100 billion in transaction volume and identified over 17 million high-risk transactions.	
Pricing Model	Subscription	
Fraud prevention partners	Accertify, CyberSource, Experian, Equifax	
Other services	N/A	
Third party connection	Accertify, CyberSource, Experian, Equifax	
Technology: anti-fraud detection tools available		
Address verifications services	Along with the email address, the billing and shipping addresses can also be passed to Emailage for a holistic risk assessment, which will help increase the fraud coverage with a higher fraud hit rate.	
CNP transactions	Yes: Emailage products are designed to be used as a up-front fraud decision for every CNP transaction where the email address is provided.	
Card Verification Value (CVV)	N/A	
Bin lookup	Yes	
Geo-location Checks	Yes: for online transactions, Emailage also receives the IP address of the transaction, which is used for Geo Location Risk Assessment, along with billing and shipping address.	
Device Fingerprint	N/A	
Payer Authentication	N/A	

Velocity Rules – Purchase Limit Rules	Yes: Emailage provides velocity controls.
White list/black list database	Yes: cross industry and cross-sector consortium database with intelligence on fraudulent emails, which is directly used on our risk decision engine and modules, to identify fraud trends, patterns, and behaviours.
KYC – Know Your Customer	N/A
Credit Rating	N/A
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities
Other	Emailage provides merchants the ability to verify the digital identity of the consumers for every transaction, making it harder for fraudsters to penetrate. So instead of the basic transaction risk assessment, email risk assessment can verify who is behind each online transaction, providing a holistic risk assessment and adding stronger controls against fraudsters while helping to approve good customers. This approach can prevent mass attacks and reduce the ability of fraudsters to scale.
Authentication Context	
Online	Yes: Emailage products are designed to be used as an up-front fraud decisioning for online transactions, they can add value every time an email address is provided on a transaction.
Mobile	N/A
ATM	N/A
POS	N/A
Call centre	N/A
other	N/A
Reference data connectivity	
Connectivity to governmental data	N/A
Other databases	Social Media Data, IP Address Geolocation & Proxy Information, Domain Attributes and Phone Ownership & Carrier Data
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	AICPA SOC 2, The EU-US and Swiss-US Privacy Shield Framework, International Association of Privacy Professionals
Regulation	N/A
Other quality programmes	N/A
Other remarks	Add other certifications
Clients	
Main clients / references	For more information contact the company.
Future developments	- digital identity verification - address demographics - real-time risk profiling - Single Sign On (SSO) - deep learning framework - enhance unsupervised learning for anomaly detection - deploy cost-sensitive machine learning model - Portal 3.0, new dashboards and user experience

RapidRisk SCORE

A lot can happen in milliseconds...

Payment fraud. Account takeover attacks. Triangulation.

That's why RapidRisk Score by Emailage is built to deliver our trusted signals in as little as 30ms* with the flexibility to handle hundreds of transactions per second.

The result? Fast, accurate fraud detection for e-commerce transactions, payment processing, charge authorizations and more.

Fast Processing Time

Average response rate is 30ms, 99% of calls are returned in 100ms or less.*

Real-Time Fraud Detection

Holistic scoring fits any workflow to maximize flexibility.

Easy System Integration

No code needed: integration takes minutes.

For more information, visit **emailage.com/rapidrisk**
or send us an email at **contact@emailage.com**

*Response time is dependent on network latency factors.

emailage®

Company	Entersekt	View company profile in online database
	Entersekt is an innovator of mobile-first fintech solutions. Financial services providers and other enterprises rely on its patented mobile identity system to provide both security and the best in convenient new digital experiences to their customers, irrespective of the service channel.	
Website	www.entersekt.com	
Keywords for online profile	mobile app security, push-based, phone-as-a-token multi-factor authentication, 3-D Secure, mobile payments, biometrics, digital transaction signing, mobile banking, online banking	
Business model	Direct and through partners	
Target market	Financial institutions, card issuers, insurers, payment service providers	
Contact	Entersekt sales team: sales@entersekt.com	
Geographical presence	Africa, Europe, Middle East, North America	
Active since	2008	
Service provider type	Digital identity service provider	
Member of industry associations and initiatives	Emerging Payments Association, FIDO Alliance, Mobey Forum, WASPA	
Services		
Core services	Mobile-app–based, multi-factor authentication and transaction signing of online banking, mobile banking, and card-not-present payments; secure biometrics enablement; mobile payments enablement platform	
Other services	Non-app-based out-of-band authentication through push USSD	
Unique selling points	Entersekt's patented emCert technology generates public/private key pairs to uniquely identify enrolled mobile devices and validate two-way communications. A self-contained cryptographic stack and communications layer enables an end-to-end encrypted channel distinct from that initiated by the device, so transactions originating from the phone can still be authenticated out of band on the same device. Highly mature and scalable, the technology is used by tens of millions of end-users globally.	
Pricing model	Per user subscription	
Partners	ABCorp, Amazon Web Services, Backbase, CREALOGIX, FIS, Global Kinetic, IBM, IST Networks, Netcetera	
Offering: authentication technology used		
Technology used	Industry-standard X.509 digital certificates; proprietary validation techniques developed specifically for the mobile phone; FIPS 140-2 Level 3 on-premise hardware appliance; dynamic public key pinning; secure browser pattern; device and application context for context-based risk scoring; advanced detection of rooting, jailbreaking, or similar mobile operating system security bypass hacks; secure enablement of fingerprint, voice, iris biometrics; SIM-swap protection; NI USSD for non-app-based out-of-band authentication	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	Yes	
Branch/Point of Sale	Yes	
Call Centre	Yes	
Other	Card-not-present payments (3-D Secure); email; staff portal; access to healthcare and insurance records; PSD2 and GDPR mandates and authorizations	

Issuing process (if applicable)	
Assurance levels conformity	N/A
Online issuing process (incl lead time in working days)	Yes: Identity proofing and enrolment processes are set by the implementing institution, but there is no reason why remote device registration should take more than a few minutes. Options available for enroling a user include phone-based registration via one-time password, scanning a printed QR code, and a combination of scanning a bank card and inputting the associated PIN.
Face-to-face issuing (incl lead time in working days)	Yes: Identity proofing and enrolment processes are set by the implementing institution, but there is no reason why in-branch device registration should take more than a few minutes.
Issuing network	Bank branches, online services
Attributes offered	
Persons Companies	Level of trust (e.g. biometric data; password or PIN; device context; geolocation and more); unique mobile device ID; digitally signed authentication message.
Reference data connectivity	
Connectivity to governmental data	Through partners in select countries;
Other databases	Mobile Connect
Certification	
Type	Entersekt's flagship product, Transakt, is FIDO Certified as a U2F (universal second factor) authenticator. Transakt is also validated with the Ready for IBM Security Intelligence program. Entersekt's card-not-present authentication solution is fully accredited by Visa, Mastercard, and American Express.
Regulation	Entersekt's solutions are engineered specifically for the heavily regulated financial sector and adhere to all major digital banking security mandates, including the requirements set out by the European Central Bank, the FFIEC, and the Monetary Authority of Singapore. They are compliant with ISO 21188:2006 (Public key infrastructure for financial services) and utilize hardware security modules certified as FIPS 140-2 Security Level 3 for encrypting and decrypting all authentication data.
Other quality programs	The underlying technology is regularly validated by independent third parties to ensure it is invulnerable to new attack vectors. The company's PSD2-compliant strong customer authentication solution to has been evaluated and approved by two European payments security consultancies.
Other remarks	
Clients	
Main clients / references	Those listed in the public domain: Absa; Bayern Card-Services; Capitec Bank; Coutts; Discovery; Ecobank; Equifax; Equity Bank; FIS; FirstBank of Colorado; Investec; Nedbank; Old Mutual; Pluscard; Swisscard. For others, please contact our sales team.
Future developments	For more information, please contact our sales team.

Company	Ethoca	View company profile in online database
ethoca™	Leveraging a growing, global network of hundreds of card issuers, and thousands of ecommerce merchants, Ethoca is the leading provider of collaboration-based technology. Their innovative solutions enable both issuers and merchants to increase card acceptance, stop fraud, recover lost revenue, and eliminate chargebacks from fraud and customer service disputes.	
Website	www.ethoca.com	
Keywords for online profile	collaboration, fraud, chargeback, card-not-present, customer disputes, protect, loss, ecommerce	
Business model	Privately held. Sell direct and through partners.	
Target market	Online shoppers, financial institutions, payment services providers, government services, online communities/web merchants, gaming and gambling, other online businesses	
Contact	sales@ethoca.com	
Geographical presence	Global (with offices in Toronto, Austin, London, Paris, Melbourne)	
Active since	2005	
Service provider type	Technology vendor, web fraud detection company, payment service provider (PSP), issuer, acquirer	
Member of industry associations and or initiatives	MRC, MAG, NRF	
Services		
Unique selling points	Ethoca's fraud and dispute intelligence is confirmed by cardholders, allowing merchants to take immediate action to stop fraudulent orders and eliminate chargebacks. Card issuers recover losses, and avoid the chargeback process. Ethoca Eliminator connects issuers to merchant order details to reduce disputes and friendly fraud, and improve the cardholder experience.	
Core services	Ethoca Eliminator, Ethoca Alerts, Enhanced Representments	
Pricing Model	More information available upon request.	
Fraud prevention partners	Kount, Accertify, CyberSource, FICO, TSYS, Lean Industries, Pega Systems, ACI	
Other services	More information available upon request.	
Third party connection	More information available upon request.	
Technology: anti-fraud detection tools available		
Address verifications services	No	
CNP transactions	Yes	
Card Verification Value (CVV)	No	
Bin lookup	No	
Geo-location Checks	No	
Device Fingerprint	No	
Payer Authentication	No	
Velocity Rules – Purchase Limit Rules	No	
White list/black list database	No	
KYC – Know Your Customer	No	
Credit Rating	No	
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities	
Other	More information available upon request.	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call centre	Yes
other	More information available upon request.
Reference Data connectivity	
Connectivity to governmental data	No
Other databases	Commercial attribute providers, e.g. credit databases
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	PCI. More information available upon request.
Regulation	PCI. More information available upon request.
Other quality programmes	More information available upon request.
Other remarks	More information available upon request.
Clients	
Main clients / references	Our suite of services delivers significant revenue growth and cost saving opportunities to more than 5400 merchants in over 40 countries and more than 580 card issuers in over 20 countries. Seven of the top ten ecommerce brands, 14 of the top 20 North American card issuers, and two of the top five UK card issuers rely on Ethoca solutions and the network that powers them.
Future developments	Additional collaboration based solutions to stop friendly fraud, minimise false declines, and increase overall acceptance.

Introducing Ethoca's

Integrated Solution Suite

Three lines of defense from genuine fraud, friendly fraud, and disputes

1 ELIMINATOR

2 ALERTS

3 ENHANCED REPRESENTMENTS

Leveraging the power of the industry's largest global merchant-issuer collaboration network, our new multi-layered Integrated Solution Suite tackles some of the biggest problems in ecommerce today and gives merchants the unique ability to:

- Eliminate chargebacks from fraud and customer disputes.
- Fight multiple forms of fraud – including friendly fraud.
- Preserve and/or recover revenue lost to fraud, disputes and chargebacks.
- Increase transaction acceptance and improve the customer experience.

Contact us today and say goodbye to fraud and chargebacks!

Company	Featurespace	View company profile in online database
FEATURE SPACE	Featurespace is the world-leader in adaptive behavioural analytics, and creator of the ARIC platform – a real-time machine learning software system for fraud management. ARIC monitors individual behaviours to catch new fraud attacks in real-time, and reduce genuine transactions declined by 70% – which could save the payments industry USD 16 bln annually.	
Website	www.featurespace.com	
Keywords for online profile	fraud, machine learning, analytics, customer friction, ARIC, adaptive analytics, real-time	
Business model	Licensed software	
Target market	Financial institutions, payment services providers, merchant acquirers, gambling and insurance	
Contact	info@featurespace.com	
Geographical presence	UK, Europe, USA	
Active since	2008	
Service provider type	Fraud detection, Technology vendor	
Member of industry associations and or initiatives	Merchant Risk Council, Network on Computational Statistics and Machine Learning	
Services		
Unique selling points	World-leading Adaptive Behavioural Analytics delivered via the machine learning ARIC platform. ARIC provides a business with a holistic view of their customers by building individual statistical profiles for every individual consumers, spotting new fraud as it occurs, simultaneously reducing genuine transactions declined by over 70%, and improving operational efficiencies by over 50%.	
Core services	Machine learning software platform for managing fraud, risk and compliance	
Pricing Model	Licence and support. For more information contact info@featurespace.com	
Fraud prevention partners	More information available upon request.	
Other services		
Third party connection	For more information email info@featurespace.com	
Technology: anti-fraud detection tools available		
Address verifications services	No	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes: more details available on request	
Bin lookup	Yes: more details available on request	
Geo-location Checks	Yes: more details available on request	
Device Fingerprint	Yes	
Payer Authentication	No	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes: more details available on request	
Credit Rating	Yes	
Follow up action	ARIC creates alerts with the capability to automate actions ie divert funds, close accounts, block cards, and more	
Other	Machine learning, behavioural analytics, in-session behaviour monitoring, link analysis, anomaly detection, sandbox functionality, deep learning models, multi-tenancy with white label UI	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	For more information please contact info@featurespace.com
POS	Yes
Call centre	For more information please contact info@featurespace.com
other	More information available upon request.
Reference data connectivity	
Connectivity to governmental data	No
Other databases	In development
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	More information available upon request.
Regulation	Regulated ICO under DPA
Other quality programmes	For more information please contact info@featurespace.com
Other remarks	For more information please contact info@featurespace.com
Clients	
Main clients / references	TSYS, WorldPay, IATA, Betfair, Danske Bank, Cortis, GoHenry, Clear Bank, MIT
Future developments	More information available upon request.

FEATURE SPACE

OUTSMART RISK

Discover the ARIC™ Fraud Hub

- Stop fraud attacks in real-time and on any device
- Increase revenue – accept more genuine customers
- Reduce customer friction by over 70%

Find out more:
www.featurespace.com

THE QUEEN'S AWARDS FOR ENTERPRISE 2018

50 Technology Fast 50 2017 UK WINNER Deloitte.

50 Technology Fast 50 2016 UK WINNER Deloitte.

CogX Best Innovation in Predictive Analytics award

FStech awards 2018 WINNER Anti-fraud or Security Solution of the Year

FT 1000 Europe's Fastest Growing Companies 2018 statista

TCPA 2018 BEST SECURITY OR ANTI-FRAUD DEVELOPMENT Category Winner

Featurespace is the world leader in Adaptive Behavioral Analytics, delivered via its machine learning ARIC™ software solution.

Contact us:
info@featurespace.com

Company	Feedzai	View company profile in online database
	Feedzai is the market leader in fighting fraud with AI. We're coding the future of commerce with today's most advanced risk management platform powered by big data and machine learning. Founded and developed by data scientists and aerospace engineers, Feedzai has one mission: to make banking and commerce safe. The world's largest banks, processors, and retailers use Feedzai's fraud prevention and anti-money laundering products to manage risk, while improving customer experience.	
Website	Feedzai.com	
Keywords for online profile	fraud, risk, protect, loss, web fraud, detection, fraud prevention, machine learning, artificial intelligence, AML	
Business model	On-premise, Cloud and Hybrid	
Target market	- issuing banks - acquiring banks - payment services providers - merchants	
Contact	sales@feedzai.com	
Geographical presence	Global	
Active since	2011	
Service provider type	Technology vendor, web fraud detection company	
Member of industry associations and or initiatives	Merchant Risk Council (MRC)	
Services		
Unique selling points	Feedzai makes commerce safe for business customers and creates a better experience for their consumers through artifcially intelligent machine learning. Financial services companies use Feedzai's anti-fraud technology to keep commerce moving safely reputation. Our unique capabilities allow customers to be efficiently removed from fraud processes, supporting merchant growth.	
Core services	Artificial intelligence and machine learning based fraud detection platform for merchants, acquirers, and issuers.	
Pricing Model	For more details contact our sales team at sales@feedzai.com	
Fraud prevention partners	More info available upon request	
Other services	Account takeover, new account registration, payment fraud prevention, frictionless authentication, bot detection, professional services	
Third party connection	More information available upon request.	
Technology: anti-fraud tools		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	No	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	Yes	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database:	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	Yes	
Follow up action	Yes	
Other	N/A	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	Yes
POS	Yes
Call centre	Yes
other	More information available upon request.
Reference Data connectivity	
Connectivity to governmental data	More information available upon request.
Other databases	More information available upon request.
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCIDSS Level 1
Regulation	Directive 95/46/EC
Other quality programmes	More information available upon request.
Other remarks	More information available upon request.
Clients	
Main clients / references	Feedzai services the world's largest global banks, merchants and processors. References are available upon request.
Future developments	More information available upon request.

FIGHT FINANCIAL CRIME WITH ADVANCED AI

LEVERAGE HYPERGRANULAR INSIGHTS

Process hundreds of millions of hypergranular Segment-of-One™ profiles in real time across you entire network

RAPIDLY ITERATE, EVEN IN PRODUCTION

Iterate on hundreds of risk models and instantaneously deploy them to production

OPERATIONALIZE ALL YOUR DATA

Ingest huge volumes of data, in any format, from any source, for a 360 degree view of your fraud exposure

feedzai

feedzai.com

Company	HID Global	View company profile in online database
	HID Global is the leading provider of trusted identity and access solutions for people, places and things. We enable organizations and enterprises in a variety of industries such as banking, healthcare, and government to protect digital identities in a connected world and assess cyber-risk in real-time to deliver trusted transactions while empowering smart decision-making. Our extensive portfolio offers secure, convenient access to on-line services and applications and helps organizations to meet growing regulatory requirements while going beyond just simple compliance.	
Website	www.hidglobal.com	
Keywords for online profile	Fraud, risk, threat detection, risk based authentication, MFA, adaptive authentication, online and mobile banking, fraud detection	
Business model	Subscription or perpetual licence	
Target market (limited list of markets)	Financial institutions, government, internal security for enterprise, US healthcare	
Contact	Olivier Thirion de Briel, othiriondebriel@hidglobal.com	
Geographical presence	Global	
Active since	1991	
Service provider type	Advanced adaptative authentication technology vendor, web fraud detection company	
Member of industry associations and initiatives	FIDO Alliance, OATH PC/SC Workgroup – https://www.pcscworkgroup.com/members/member-list/ Smart Card Alliance – https://www.securetechalliance.org/alliance-members/2702/ GlobalPlatform – https://www.globalplatform.org/membershipcurrentfull.asp Open Identity Exchange (OIX) http://oixuk.org/members/ Note OIX also runs OpenID – IdenTrust, part of HID Global, is a general member UK Finance https://www.ukfinance.org.uk/ – IdenTrust, part of HID Global, is an Associate Member Open Banking https://www.openbanking.org.uk/ – IdenTrust is an active participant in the development of Open Banking standards in the UK Open Banking Stakeholder Group Membership PSD2/RTS Implementation Third Parties Open Banking Working Group Membership Customer WG; Information Security WG; Regulatory & Legal WG Standards WG; Operational Governance Agreement and Services WG	
Services		
Unique selling points	HID Global empowers banks to create trusted environment for digital transactions along with frictionless user experience based on push notification with highest security level thanks to the use of public key cryptography and embedded mobile application security functionalities. We deliver advanced adaptive authentication, highly secure and easy to deploy fully compliant with the PSD2 and Open Banking requirements. The combination of evidence-based threat detection capabilities, anomaly detection and behavioural biometrics supported by machine learning makes it unique on the market. Our Professional Services team ensures effective deployment and decrease organization's time to market.	
Core services	Online and mobile banking protection, strong customer authentication, dynamic linking, transaction signature, threat and fraud detection, multi factor authentication, behavioural biometry, facial and fingerprint biometry	

Pricing	Pricing is per user and based on volume and number of protected channel
Partners	Temenos, Thales, Microsoft
Other services	Globally trusted certificate authority, credential management solution for high assurance needs, physical identity, and access management solution
Offering: authentication technology used	
PIN	Yes
Password/phrase	Yes
Token	Yes
Card	Yes
Digital certificates (hosted yes/no)	Yes
Multifactor authentication	Yes
Biometrics	Yes
Authentication context	
Online	Yes
Mobile	Yes
ATM	Yes
Branch/Point of Sale	Yes
Call Centre	Yes
Other	Payment channel, internal security use cases
Reference data connectivity	
Connectivity to governmental data	No
Other databases	No
Certification	
Type	ANSSI CSPN, FIPS 140-2, ISO 27001, ETA Jan 19
Regulation	Open Banking UK, PSD2, PCI-DSS 3.2, 23 NYCRR 500, GDPR
Other quality programs	For more information contact the company – Thirion de Briel, Olivier <othiriondebriel@hidglobal.com>
Other remarks	For more information contact the company – Thirion de Briel, Olivier <othiriondebriel@hidglobal.com>
Clients	
Main clients / references	For more information contact the company – Thirion de Briel, Olivier <othiriondebriel@hidglobal.com>
Future developments	Widening its biometric offering and enhancing threat and fraud detection capabilities.

PROTECT DIGITAL IDENTITIES AND ACCURATELY ASSESS RISK

TO EMPOWER SMART DECISION-MAKING.

With the increase of online activities it is essential to be able to assess the level of risk when authenticating digitally. Through data analysis powered by machine learning and artificial intelligence the level of risk can be assessed and a real-time decision engine will enable organizations to manage it and define the authentication steps according to the circumstances. This way, they can effectively protect both employees within the company and their customers.

You'll call it innovation in authentication. We call it, *powering trusted identities.*

Powering **Trusted Identities** | Visit us at hidglobal.com/hidrms

Company	iovation, a TransUnion company	View company profile in online database
	iovation, a TransUnion company, was founded in 2004 to make the Internet a safer place to conduct business. iovation protects online brands from cybercriminal activity with online fraud prevention and consumer authentication solutions. Having the world's largest database of reputation insights iovation safeguards tens of millions of transactions each day.	
Website	www.iovation.com	
Keywords for online profile	device identification, device reputation, online fraud prevention, online fraud detection, mobile fraud, account takeover prevention, device-based authentication, customer authentication, online reputation, multifactor authentication, device fingerprinting	
Business model	SaaS	
Target market	Online businesses such as retailers, financial institutions, lenders, prepaid cards, insurers, social networks and dating sites, logistics, gaming/MMO, gambling operators, online auction sites, and travel and ticketing companies.	
Contact	Connie Gougler, Director of Marketing, connie.gougler@iovation.com, 503-943-6748	
Geographical presence	Global: iovation's business is 51% US and 49% international	
Active since	2004	
Service provider type	Device intelligence, fraud detection & prevention, customer authentication, multifactor authentication	
Member of industry associations and or initiatives	Merchant Risk Council, Online Lenders Association	
Services		
Unique selling points	iovation provides a frictionless, flexible, reliable, real-time SaaS solution for user authentication and fraud prevention that tells our clients if a customer visiting their site is authorized for that account and/or is risky based upon specific criteria for evaluating the transaction or activity. iovation's global consortium contains the reputations of four billion devices and 55 million fraud events such as chargebacks, identity theft, account takeovers, online scams and many more.	
Core services	iovation offers fraud prevention, customer authentication, multifactor authentication, and transaction reputation scoring	
Pricing Model	Per transaction fee based on system usage depending on volume, type of transaction, and length of contract.	
Fraud prevention partners	4Stop, ACI Worldwide, Avoka, Dealflo, Entrust Datacard, Equifax, Fischer International, Fiserv, Playtech, Regily, Scudetto, Synectic Solutions, TransUnion, TruNarrative	
Other services	Our clients have access to the Fraud Force Community, an exclusive private B2B network of the world's foremost security experts sharing intelligence about cybercrime prevention, device identification, new threats and other fraud-related topics.	
Third party connection	iovation delivers data in XML format and offers real-time APIs, allowing output to be integrated easily with third-party systems	
Technology: anti-fraud detection tools available		
Address verifications services	No: While we do not offer AVS services, we capture the IP address and its geolocation of the device in the transaction. We can flag transactions from 'blocked' countries, as well as notify clients when mismatches occur between the IP address shown by the user's browser and the IP address we collect with our Real IP proxy unmasking feature.	
CNP transactions	Yes: iovation's service is primarily used to detect high risk activity at login, account creation, fund transfer and checkout. In addition, our iovation score helps identity the most trustworthy customers in our clients' review queues so that they can take good business immediately, and offer higher-value promotions to their preferred customers.	
Card Verification Value (CVV)	No: This service is handled through our client's payment processor.	
Bin lookup	No: This service is handled through our client's payment processor.	
Geo-location Checks	Yes: iovation's clients can flag transactions when activity is coming from an unauthorized country or through a proxy, and they can use our Real IP technology to pinpoint the user's actual location.	

Device Fingerprint	Yes: iovation offers a defense-in-depth approach to device recognition, supporting native and web integrations for mobile, tablet and desktop devices.
Payer Authentication	No: This service is handled through our client's payment processor.
Device-based Authentication	Yes: iovation's authentication service allows clients to use their customer's known devices to help verify identity. Authentication happens in real-time, behind the scenes, reducing unnecessary friction.
Velocity Rules – Purchase Limit Rules	Yes: iovation's velocity rules flag transactions when thresholds are exceeded. These may include situations where too many accounts are accessed per device, or too many new accounts are created within a timeframe. Specific rules include Accounts per Device, Accounts Created per Device, Countries per Account, Countries per Device, Transactions per Account, and Transactions per Device. Our service also flags transaction value thresholds, and other transactional velocities.
White list/black list database	Yes: iovation clients can flag transactions based on custom-built lists. These can be positive or negative lists. List types include accounts, devices, IP ranges, ISPs, locations and others, and are easily managed across rule sets.
Device Anomalies	Yes: iovation clients can flag transactions when device settings are anomalous and indicative of risk. While individual device characteristics may not be proof of risk, certain characteristics may be worth monitoring, and several in combination with each other may indicate attempts by the user to evade detection.
Fraud and Abuse Records	Yes: iovation clients can flag transactions that originate from an account or device already associated with fraud or abuse. Previous fraud or abuse is recorded in our system as evidence. The customer sets the types of evidence they want to consider, and decides whether to leverage only the evidence they log, or consider the evidence of other iovation subscribers.
KYC – Know Your Customer	No
Credit Rating	No
Follow up action	iovation's fraud prevention service provides an Allow, Review or Deny result for each transaction. Clients then decide the best course of action to take in response to these results. iovation also returns detailed information about the device associated with the transaction; clients can store this data and correlate it back to identity management and other systems as needed.
Authentication Context	
Online	Yes
Mobile	Yes: iovation's mobile SDK for iOS and Android identifies jailbroken or rooted devices, and captures device location through IP address, network-based geo-location information, and GPS data. The location services expose mismatches between the reported time zone and location, long distances between transactions made in short periods of time, and other location-based anomalies. It also detects transactions originating from virtual machines or emulators.
ATM	Yes: iovation's device-based multifactor authentication solution can be used to facilitate the authentication of a person at an ATM.
POS	Yes: iovation's device-based multifactor authentication solution can be used to facilitate the authentication of a person at POS.
Call centre	Yes: iovation's device-based multifactor authentication solution can be used to facilitate the authentication of a person contacting a call centre.
Reference data connectivity	
Connectivity to governmental data	No
Other databases	Neustar – IP geolocation
Fraud management system type	
Single-channel fraud prevention system	Yes: iovation delivers comprehensive online fraud prevention and customer authentication for mobile, tablet and PC-based transactions.
Multi-channel fraud prevention system	Our services focus on online transactions and complement a multi-channel prevention system.

Certification	
Type	iovation is Privacy Shield certified and is SOC 2 compliant as of April 2, 2018.
Regulation	iovation supports FFIEC compliance by providing device identification and device-based authentication services.
Other quality programmes	iovation follows strict Quality Assurance processes for new products and services, and offers Service Level Agreements (SLAs) which include 99.9% uptime as a part of all customer agreements.
Other remarks	For more information, please contact iovation at info@iovation.com
Clients	
Main clients / references	Ikano Bank UK, UMB Bank, NASA Federal Credit Union, 4Finance, Gain Capitol, The AA, Gocompare, B&H Photo, Bazaarvoice, No Office Walls, and hundreds more.
Future developments	For more information, please contact iovation at info@iovation.com

Company	iSignthis	View company profile in online database
	iSignthis is a leading e-money, payments, and identity technology company, publicly listed on the Australian Securities and Frankfurt Stock Exchange (ASX: ISX | FRA: TA8). Through our patented Paydentity and ISXPay solutions, we enable online businesses to stay on top of the regulatory curve whilst also optimising their payment cycle, in a safe, comprehensive, and cost-effective way.	
Website	www.isignthis.com	
Keywords for online profile	identity verification, authentication, payment gateway, payment processing, card acquiring, e-money issue and redemption, fraud and risk management	
Business model	B2B, transactional	
Target market	Online businesses with specific focus on high-risk/AML regulated sector merchants where (enhanced) Customer Due Diligence KYC is a regulatory requirement. Our solutions are also utilised by merchants seeking to mitigate fraud and chargebacks.	
Contact	contact@isignthis.com	
Geographical presence	Global	
Active since	2013	
Service provider type	E-money, identity verification, and payments technology company	
Member of industry associations and or initiatives	ECSG, EPC, EPSM, OIX	
Services		
Core services	The company's core services include: Paydentity, which converges real time processing, clearing, and settlement with verification of payment instruments, delivering AML/CFT KYC identification of customers, payments and transaction monitoring simultaneously from a single platform. iSignthis, trading as ISXPay, also offers merchant card acquiring and payment services as an EEA authorised e-money Monetary Financial Institution, as well as transactional banking services including B2B EU based e-money accounts.	
Unique selling points	Paydentity combines the verification of the end-user's identity with the processing of their payment transaction, to simultaneously satisfy both AML/CFT regulatory requirements whilst clearing payments on behalf of the merchant. Our unique solution protects both online customers/cardholders from fraud whilst also protecting merchants against chargebacks. We deliver compelling evidence to reverse chargebacks and offer CNP liability shift under the incoming EU's PSD2.	
Pricing Model	Transactional	
Fraud prevention partners	N/A	
Other services	Find more information about our products by visiting our website or contacting our team, sales@isignthis.com	
Third party connection	Principal of Visa, Mastercard, AMEX, JCB, UnionPay in Europe and Australia, with a number of partner networks spanning the rest of the world	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	Yes	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	Yes	

Follow up action	Payment instrument verification, two-factor authentication, mobile OTP
Other	N/A
Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call centre	No
other	N/A
Reference data connectivity	
Connectivity to governmental data	Yes: globally
Other databases	Additional information available upon request
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCI DSS 1, ISO 27001
Regulation	Licensed/regulated in both Australia and the European Economic Area to process, clear, and settle payments
Other quality programmes	SWIFT BIC: ISEMCY22, CBC EMI License # 115.1.3.17 (passported to all EEA states)
Other remarks	N/A
Clients	
Main clients / references	Top tier high-risk merchants in the financial services, adult, gaming, gambling sectors as well as a range of money and payment service providers
Future developments	- strengthen our established iSXPay platform by expanding our Tier 1 connections across geographies and partner networks - utilise our e-money license in conjunction with our other products to offer additional transactional banking capabilities to our merchants - continue our strategic acquisitions like our recent one of Probanx, which currently supplies core banking software to banks across three continents

iSignthis®

The complete transactional banking ecosystem for digital businesses.

We enable your business to satisfy all your payment and identity needs, by using next-generation technology and a compliance-first approach.

Identity Platform

From enhanced due diligence KYC, to our patented Paydentity™ process, we offer a dynamic, real-time solution for verifying the identity of your customers willing and able to pay for your services.

Payment Platform

Advanced payment processing from all major card schemes like VISA, Mastercard, AMEX and JCB as well as card acquiring with multi-connected partnerships spanning across the world.

Banking Platform

Transactional banking services for the modern business. Business accounts and eWallets made easy for you and your customers with a number of payouts options available including SWIFT, SEPA and OCT.

iSignthis® (ASX: ISX | FRA: TA8) is a leading payment and identity technology company.

iSignthis eMoney Ltd is a licensed E.E.A Monetary Financial institution authorized and supervised by the Central Bank of Cyprus #115.1.3.17.

EEA Authorised EMI #115.1.3.17 | ASX | BÖRSE FRANKFURT | ico. | PRINCIPAL MEMBER: VISA | AGGREGATION PARTNER: AMEX

Company	Kount	View company profile in online database
	Kount's award-winning fraud management, identity verification and online risk detection technology empowers digital businesses, online merchants and payment service providers around the world. With Kount, businesses approve more orders, uncover new revenue streams, and dramatically improve their bottom line all while minimising fraud management cost and losses. Kount delivers certainty in every digital interaction.	
Website	www.kount.com	
Keywords for online profile	fraud prevention, account takeover, payment security, ecommerce, AI, machine learning, merchant network, authentication	
Business model	SaaS	
Target market	ecommerce, financial institutions, payment services providers, online communities, web merchants, apparel, automotive, quick serve restuarants, loyalty, digital streaming, electronics, food/beverage, health/beauty, home/kitchen, gaming/gambling, telecom, travel/leisure, other online and card not present businesses	
Contact	fraudfighter@kount.com	
Geographical presence	Worldwide	
Active since	2007	
Service provider type	SaaS technology vendor, web fraud detection company	
Member of industry associations and or initiatives	Merchant Risk Council, National Retail Federation, CPE Credit Certification by NASBA, Internet Merchants Retail Group, Global Retail Insights Network.	
Services		
Unique selling points	Through Kount's global network and proprietary technologies in AI and machine learning, combined with policy and rules management, customers thwart online criminals and bad actors. Kount's continuously adaptive platform provides certainty for businesses at every digital interaction.	
Core services (Max 20 words)	Kount's proprietary techniques and patented technology, including: superior mobile fraud detection, machine learning, feature engineering, multi-layer device fingerprinting, IP proxy detection and geo-location, transaction and custom scoring, global order linking, business intelligence reporting, comprehensive order management and professional services	
Pricing Model	Tiered SaaS-based pricing model	
Fraud prevention partners	- Channel Partners: BlueSnap, Braintree (a PayPal Service), Cayan, Chase, Conekta, Etisalat, Eway, First Atlantic Commerce, Global Payroll Gateway, J.P. Morgan, LimeLight, MaxiPago, Moneris, Openpay, PayCertify, Pinpoint Intelligence, Recurly, Sage - Ecommerce Partners: 3dcart, demandware, Magento, mozu, Pulse Commerce, Xcart	
Other services	Chargeback managed services, risk-based authentication, fingerprinting, data orchestration, quarterly business review, policy/rules management, sales and marketing support (Kount Central Product), DataMart business intelligence, comprehensive onboarding and ongoing training support, dedicated client success manager, service support knowlege base.	
Third party connection	BehavioSec, Chargebacks 911, Ethoca, LexisNexis, Neustar, TeleSign, WhitepagesPro.	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	No	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	No	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	

Credit Rating	No
Follow up action	Robust APIs and case management to trigger any type of follow up action.
Other	Complete case management, agent management and reporting, mobile SDK for superior device authentication, mobile app and mcommerce fraud prevention, supervised and unsupervised machine learning.
Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call centre	Yes
other	In-store kiosk, mail order, omnichannel.
Reference data connectivity	
Connectivity to governmental data	No
Other databases	WhitepagesPro, BehavioSec
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCI Compliance Level 1 Service Provider and Participating Organization, SOC 2 Type II, Privacy Shield, GDPR.
Regulation	More information available upon request
Other quality programmes	More information available upon request
Other remarks	Contact fraudfighter@kount.com for more information.
Clients	
Main clients / references	CD Baby, Crate & Barrel, Domino's Pizza, Dunkin' Brands, Hydrobuilder, Jagex, JOANN Fabric & Crafts, Leatherman, Micro Center, PetSmart, Staples, The Iconic, The Source, The Vitamin Shoppe, TickPick, WebJet, and more.
Future developments	Kount is continuously delivering net new functionality month after month, contact fraudfighter@kount.com for more information.

Increase Sales with Better Fraud Protection

Get back to business and let Kount take fraud off your hands.

Digital businesses using Kount have the confidence to grow boldly. How? Kount aggregates billions of transactions through its global network, feeding its AI and machine learning to expose fraud more accurately than other systems, in milliseconds. Weigh the value of each customer against potential fraud risk to maximize conversions with Kount.

Learn more about Kount's powerful tools for online retailers at **www.kount.com**

Kount®

Boost Sales. Beat Fraud.

Company	Melissa	View company profile in online database
	Melissa is a leading provider of electronic identity verification, entity resolution and global contact data quality. Since 1985, we've helped more than 10,000 organisations worldwide to achieve and maintain quality data for a single, accurate and reliable customer view. Melissa's solutions help companies operate more efficiently, deliver outstanding customer service and minimise risk.	
Website	www.melissa.com	
Keywords for online profile	eIDV, KYC, identity verification, contact data, payment, fraud detection	
Business model	Real-time API integration and cloud-based	
Target market	Card issuers, payment processors, financial institutions, payment services providers, government services, online communities/web merchants, gaming and gambling, other online businesses	
Contact	sales@melissa.com	
Geographical presence	Global	
Active since	1985	
Service provider type	Web fraud detection company, digital identity service provider and technology vendor	
Member of industry associations and or initiatives	Armed Forces Communications and Electronics Association (AFCEA)	
Services		
Unique selling points	Real-time integration allows you to verify that your customer is who they say they are in seconds. Melissa's services speed up customer onboarding and simplify checkout while minimising the risk of fraud and helping you stay compliant with industry regulations.	
Core services	Cloud-based identity resolution (national ID and age verification, watch list/PEP screening, contact data validation), location intelligence and consumer insights	
Pricing Model	Annual subscription based on volume	
Fraud prevention partners	Scannovate	
Other services	Optical character recognition (OCR) and data quality solutions that verify, standardise, update, enrich and dedupe data.	
Third party connection	Scanovate	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	No	
Bin lookup	No	
Geo-location Checks	Yes	
Device Fingerprint	No	
Payer Authentication	Yes	
Velocity Rules – Purchase Limit Rules	No	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	No	
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities	
Other	Person and company authentication for name, address, phone, email, national ID, location, demographics and IPv4 information	
Authentication Context		
Online	Yes	
Mobile	Yes	
ATM	No	

POS	No
Call centre	Yes
other	For more information, please contact the company.
Reference data connectivity	
Connectivity to governmental data	International government data sources
Other databases	Credit, consumer, commercial, telco, utility, and other proprietary data sets
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	SOC 2 type II, HIPAA/HITECH, US/EU privacy shield, USPS® CASSTM and Canada Post® SERP CertifiedTM
Regulation	KYC, anti money laundering (AML), Bank Secrecy Act (BSA)
Other quality programmes	Primary compliance, fraud prevention, watchlist screening/Politically Exposed Persons (PEP)
Other remarks	Melissa operates numerous redundant, distributed server farms across the globe to ensure 99.99% uptime. Beyond the 99.99%, we offer service level agreements (SLAs) for those who need them. Our RESTful API provides data in both XML and JSON, and features SSL 256-Bit Encryption.
Clients	
Main clients / references	Bank of America, Citi Bank, US Bank, Discover, Volvo Car Financial Services, Sun Trust, Meta Bank, car2go
Future developments	For more information, please contact the company.

JOIN THE EIDV REVOLUTION

Fight Fraud & Declare Independence from Untrusty Identities

Losing money each year to fraud and compliance costs? Join the fight! Break free from bad contact data with Melissa. We offer affordable solutions that quickly provide real-time electronic ID verification – so you know who you're doing business with, at the time you're conducting business – every time.

- Real-time global ID verification
- National ID, age & name-to-address check
- Mobile identity management with OCR
- Demographic & location data enrichments
- PEP & international watch list screening

See how Melissa eIDV solves your specific business needs.
Request a Free Demo.

Melissa.com/revolution
1-800-MELISSA

melissa®

Company	RISK IDENT	View company profile in online database
	RISK IDENT is an anti-fraud software development company based in the US and Europe that protects companies within the ecommerce, telecommunication, and financial sectors. RISK IDENT's machine-learning software uses sophisticated data analytics to block any kind of fraud, all with human-friendly user interface that simplify a fraud prevention team's decision-making process.	
Website	www.riskident.com	
Keywords for online profile	online fraud prevention, account takeover prevention, device indentification, worlwide device pool, automatic fraud detection, fraud case processing, credit risk evaluation, mobile SDK	
Business model	Direct and through partners	
Target market	- online merchants - financial institutions - payment services providers - online communities - gaming and gambling - other online businesses	
Contact	contact@riskident.com	
Geographical presence	Global	
Active since	2013	
Service provider type	- technology vendor - fraud detection	
Member of industry associations and or initiatives	Merchant Risk Council	
Services		
Core services	RISK IDENT battles payment fraud and account takeovers with a collection of highly developed software products that are easy to integrate. The software applies algorithms and machine learning on different data feeds to identify fraud risks on a variety of devices. FRIDA is an intelligent all-in-one solution that analyses transactions using data analytics and machine-learning. It will continuously adapt to changing fraud patterns. DEVICE IDENT, a sophisticated device fingerprinting technology on the market, uses efficient rule sets that calculate a risk score to every device – including a SDK for native mobile applications.	
Core services	- fraud detection and credit scoring software - device fingerprinting services	
Pricing Model	Monthly licensing fees (FRIDA)/Per transaction (DEVICE IDENT)	
Fraud prevention partners	For more information please contact the company	
Other services	For more information please contact the company	
Third party connection	Yes	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	No	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	No	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	Yes	
Follow up action	Various	
Other	For more information please contact the company	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	Yes
Call centre	No
other	For more information please contact the company
Reference data connectivity	
Connectivity to governmental data	No
Other databases	Identity and address providers, credit scoring providers
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	For more information please contact the company
Regulation	For more information please contact the company
Other quality programmes	For more information please contact the company
Other remarks	Fully EU data privacy compliance
Clients	
Main clients / references	Key investor is Otto Group, Europe's biggest online retailer
Future developments	For more information please contact the company

DOES FRAUD AFFECT YOUR BUSINESS?

Think like a fraudster and fight the bad guys!

Safeguard your enterprise and your customers by halting the sophisticated strategies of fraudsters and minimizing false positives – both of which boost sales.

We believe every business should have the most up-to-date technology in the fight against fraud. Stop fraudsters in their tracks and simultaneously create a better customer experience with RISK IDENT. As global experts with long-term experience in data science and machine learning, we offer highly efficient anti-fraud solutions that protect millions of transactions within e-commerce, telecommunications and financial services – each and every day.

RISK IDENT

www.riskident.com | **contact@riskident.com**

Company	RSA	View company profile in online database
	RSA, a Dell Technologies business, offers business-driven security to help organisations manage digital risk and protect what matters most. Award winning cybersecurity solutions from RSA can detect and respond to advanced attacks, manage user identities and access, and reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to rsa.com.	
Website	www.rsa.com	
Keywords for online profile	fraud detection, fraud prevention, consumer authentication, adaptive authentication, 3-D Secure, CNP transactions, account takeover, PSD2	
Business model	Direct and partners	
Target market	- financial institutions - payment services providers - card issuers - insurance and brokerages - ecommerce	
Contact	https://www.rsa.com/en-us/contact-us 800-995-5095	
Geographical presence	North America, Europe, Middle East, Africa, AsiaPac, India, LATAM, Japan	
Active since	1982	
Service provider type	- technology vendor - web fraud detection company	
Member of industry associations and or initiatives	FS-ISAC, NACHA, U.S. Payments Forum, NEACH, EMVCo, National Cybersecurity Alliance	
Services		
Unique selling points	Omnichannel support: organisations can send RSA Adaptive Authentication details of transactions outside of the traditional web and mobile channels for risk assessment. **Fraud detection rates:** achieve 95% fraud detection rate with less than 5% requiring step-up authentication. **The RSA eFraudNetwork:** is a global cross-organisational database of confirmed fraud data gathered from an extensive network of RSA customers, ISPs, and third-party contributors worldwide. The eFraudNetwork is one of the many factors that contribute to the RSA Risk Engine in determining fraud risk. **Transaction Signing:** RSA Adaptive Authentication offers transaction signing, which can optionally integrate with biometrics as a stronger means of authentication layered on top of the payment transaction signature.	
Core services	RSA Adaptive Authentication is an advanced, omni-channel fraud detection hub that provides risk-based, multi-factor authentication for organisations seeking to protect their consumers from fraud across digital channels. Powered by the RSA Risk Engine, RSA Adaptive Authentication is designed to measure a user's login and post-login activities by evaluating a variety of risk indicators. Using powerful machine learning, in company with options for fine-grained policy controls, the RSA Adaptive Authentication anti-fraud hub only requires additional assurance, such as out-of-band authentication, for scenarios that are high risk and/or violate rules established by an organisation. This methodology provides transparent authentication for the majority of the users, ensuring a positive user experience.	
Pricing Model	RSA Adaptive Authentication can be purchased in an On-Premise or Cloud deployment. - On-Premise: user-based; supports both Perpetual and Subscription licenses - Cloud: transaction-based; supports Subscription licenses - Perpetual user licenses: once the customer pays for them, they are theirs for perpetuity, no additional payment required ever - Subscription user licenses: these are paid for a pre-determined time; at the end of that time, the user must renew their subscription. Maintenance is included. - Software maintenance: this is tied to the perpetual user licenses. This is a yearly renewable cost based on the number of user licenses that customer owns. The software maintenance allows for customer support, upgrades, and access to RSA's extensive knowledge base.	

Fraud prevention partners	Partners include, but are not limited to: Jack Henry, FiServ, TODO1, ACI, & FIS
Other services	Out of Band SMS/Phone integration partners include Telesign & Authentify
Third party connection	If a customer is interested in integrating data elements from an existing third-party relationship, they may do so by utilising the ecosystem approach. Through the RSA Adaptive Authentication ecosystem approach, organisations can use the RSA Risk Engine to consume external data elements, in addition to RSA's predefined facts, to calculate a risk score. By utilising 3rd party facts to influence the risk assessment and impact the risk score, customers can contribute additional insights from both internal business intelligence and additional anti-fraud tools.
Technology: anti-fraud detection tools available	
Address verifications services	Yes: can facilitate a billing address (AVS) check via RSA Adaptive Authentication for eCommerce with issuer/processor.
CNP transactions	Yes: only with the issuer/issuing processor side
Card Verification Value (CVV)	Yes: can consume and verify as part of RSA Adaptive Authentication for eCommerce.
Bin lookup	Yes: can verify fraud tied to a BIN or specific card number as part of RSA Adaptive Authentication for eCommerce.
Geo-location Checks	Yes: part of the RSA Risk Engine in both RSA Adaptive Authentication and RSA Adaptive Authentication for eCommerce.
Device Fingerprint	Yes: part of the RSA Risk Engine in both RSA Adaptive Authentication and RSA Adaptive Authentication for eCommerce.
Payer Authentication	Yes: part of RSA Adaptive Authentication for eCommerce (3-D Secure ACS service)
Velocity Rules – Purchase Limit Rules	Yes: can deploy in rules in both RSA Adaptive Authentication and RSA Adaptive Authentication for eCommerce.
White list/black list database:	Yes: can facilitate these in both RSA Adaptive Authentication and RSA Adaptive Authentication for eCommerce.
KYC – Know Your Customer	No
Credit Rating	No
Follow up action	Breadth of Step-up authentication modalities, paired with the flexibility of the Multi-Credential Framework: - biometrics: fingerprint and face ID - transaction signing - SMS/Phone call - push notification - challenge questions - knowledge-based authentication (KBA) - OTP - email - multi-credential framework: third-party authentication methods can be integrated via the RSA Multi-Credential Framework, such as tokens (like RSA SecurID) or card readers
Other	IP address, Known Bad IP, Geo-Velocity, Device Type, cookie, device health assessment (i.e. RSA Adaptive Authentication RDP Trojan Protection), Device history, User Attributes, User History, new device check, jailbroken/rooted device
Authentication Context	
Online	Yes
Mobile	Yes
ATM	Yes
POS	No
Call centre	Yes
other	IVR, custom IOT channel

Reference Data connectivity	
Connectivity to governmental data	Not out of the box. However, a customer can integrate a data store via the RSA Adaptive Authentication "ecosystem approach", to contribute new data elements in the form of risk score custom facts.
Other databases	RSA eFraudNetwork. The RSA eFraudNetwork is a global cross-organisational database of confirmed fraud entities gathered from an extensive network of RSA customers, ISPs, and third-party contributors worldwide. When fraudulent activity is identified, the data elements associated with this activity, such as device or payee, are shared via the RSA eFraudNetwork. When RSA Adaptive Authentication identifies a mule account, an account used to transfer funds that have been obtained fraudulently, it is flagged as high-risk and the mule account details are shared through the RSA eFraudNetwork service. The RSA eFraudNetwork service provides direct feedback to the RSA Risk Engine, so that future transactions or activities attempted from a device or IP address that appears in the RSA eFraudNetwork service data repository are classified as high risk. In addition, through the RSA Adaptive Authentication ecosystem approach, an organisation can consider the database of their choice, to influence the risk assessment: Through the RSA Adaptive Authentication ecosystem approach, organisations can use the Risk Engine to consume data elements, in addition to RSA's predefined facts, to calculate a risk score. By utilising third party facts to influence the risk assessment and impact the risk score, customers can contribute additional insights from both internal business intelligence and additional anti-fraud tools.
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	
Regulation	- RSA Adaptive Authentication: GDPR - RSA Adaptive Authentication for eCommerce: PCI DSS, EMVCo
Other quality programmes	For more information, contact RSA
Other remarks	For more information, contact RSA
Clients	
Main clients / references	Financial services, insurance, brokerages, ecommerce, healthcare
Future developments	RSA Forward Looking Statements Notice: concepts presented for consideration only. RSA makes no representation and undertakes no obligations with regard to product planning information, anticipated product characteristics, performance specifications, or anticipated release dates (collectively, "Roadmap Information"). Roadmap Information is provided by RSA as an accommodation to the recipient solely for purposes of discussion and without intending to be bound thereby. Copyright 2017 Dell Technologies Corp. All rights reserved. - Enhanced omnichannel strategy – support for the ingestion of raw data across channels in addition to enriched data. - Improved Risk Scoring with deep entity profiling – to create a more accurate profile of consumers by leveraging insight into consumers online banking and ecommerce activities, web-session intelligence and recovered compromised data from deep-web sources. The combined information will ultimately lead to stronger fraud detection rates and lower false positives. - eFraudNetwork Global Community Intelligence Sharing Enrichment – community data sharing platform will be enriched by extending consumers' behavioural patterns outside of one single customer and expand the types of data/knowledge that is shared, including recommendations on policy settings derived from like-sized entities. - Easing the integration process will lower customers TCO (resources needed to integrate) and allow easier implementations allowing smaller organisations to perform more self service. - Automated case/alert handling – to help customers deal with growing caseloads and as a result, reduce TCO.

RSA BUSINESS-DRIVEN SECURITY™

STOP FRAUD NOT CUSTOMERS

FRAUD PREVENTION SOLUTIONS THAT MEAN BUSINESS

PURSUE DIGITAL OPPORTUNITIES WITH CONFIDENCE

Digital transformation presents many new opportunities—and unintended risks. Fraud does not have to be one of them. The RSA® Fraud & Risk Intelligence Suite enables you to manage fraud risk and digital threats across your omnichannel business, without compromising your customers' experience.

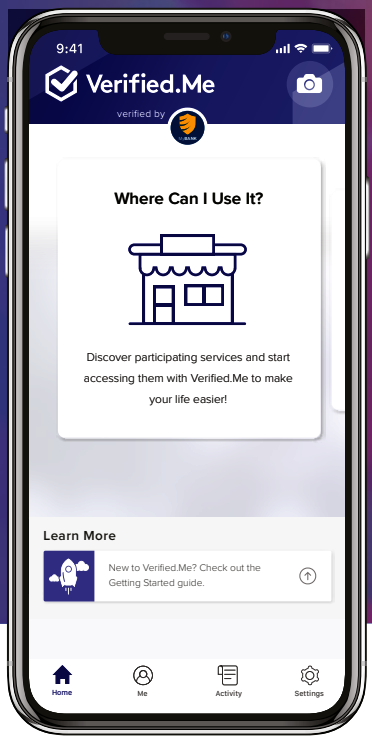
Digital business begins with the RSA Fraud & Risk Intelligence Suite, offering the industry's highest fraud detection rates without blocking legitimate customers and transactions. With the RSA Fraud & Risk Intelligence Suite, you never have to sacrifice your customers' security for their convenience.

For more information, visit **rsa.com/fraudprevention**

Company	SecureKey Technologies	View company profile in online database
	SecureKey is a leading identity and authentication provider that simplifies consumer access to online services and applications.	
Website	www.securekey.com	
Keywords for online profile	digital Identity, authentication, blockchain	
Business model	Info upon request	
Target market	Info upon request	
Contact	info@securekey.com	
Geographical presence	Global	
Active since	2009	
Service provider type	Digital identity service providers	
Member of industry associations and initiatives	DIACC, OIX, FIDO, Hyperledger, GPS, IDPro, Kantara	
Services		
Core services	SecureKey Concierge and Verified.Me	
Other services	E.g. transaction services: offering connectivity to other credential issuers	
Unique selling points	Verified.Me, by SecureKey Technologies, is a new service to help you verify your identity, so you can get things done fast online, in person and on the phone. Verified.Me helps you verify your identity quickly and securely from any iOS or Android smartphone, using personal information that you consent to share from your connections. You always stay in control by choosing when to share your information and with whom, reducing unnecessary oversharing of personal information in order to access the services you want. The Verified.Me service is protected with strong security protocols to prevent personal information from being identified, accessed or misused. Verified.Me uses blockchain technology to securely and privately transfer your personal information to trusted network participants, giving you easy access to the services you want, when you want them. Contact us today to learn more about joining our growing network.	
Pricing model	N/A	
Partners	See full list here: https://securekey.com/partner-directory/	
Offering: authentication technology used		
Technology used	Info upon request	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	Info upon request	
Branch/Point of Sale	Info upon request	
Call Centre	Info upon request	
Other	Info upon request	

Verified.Me™

An ecosystem approach to verifying digital identity



SECURE KEY

Verified.Me is the new and secure way to help you verify your identity, so you can quickly get access to the services and products you want online, in person and on the phone.[1]

Visit www.securekey.com/join us to learn more.

[1]Some features are not yet available. |

Company	Sedicii	View company profile in online database
	In the world of regulated digital services Sedicii delivers robust, efficient, and fast customer onboarding services in full compliance with the most stringent CDD, KYC, AML, and Data Privacy obligations. Sedicii's Zero knowledge proof technology provides state-of-the-art capability for real-time identity verification against trusted identity providers that is completely privacy preserving.	
Website	https://sedicii.com/	
Keywords for online profile	digital identity, remote onboarding, e-Identity, real-time authentication, AML, KYC, AMLD5, PSD2, fraud detection	
Business model	Subscription-based, transaction-based	
Target market	Financially regulated industries: financial institutions, governments, legal and accounting, retailing/merchants, telco, and more	
Contact	contactus@sedicii.com	
Geographical presence	Global	
Active since	2013	
Service provider type	Privacy preserving identity authentication and verification services	
Member of industry associations and initiatives	World Economic Forum, FIDO Alliance	
Services		
Unique selling points	Sedicii's streamlined identity authentication and verification network uses advanced ZKP technology. It enables verification of identity attributes without data being exposed or exchanged, thereby ensuring that both the privacy of the individual, and the confidentiality and integrity of the Identity Providers' data remains intact.	
Core services	Secure account creation, robust, secure, real-time KYC/AML/GDPR compliant onboarding document/information capture, identity proofing, background checks, risk profiling, live video interview	
Pricing Model	Subscription-based, transaction-based	
Fraud prevention partners	For more information contact the company	
Other services	Identity Verification against Identity Providers connected to the network eliminates data exposure during the checking process	
Offering: authentication technology used		
PIN	Yes	
Password/phrase	Yes	
Token	Yes	
Card	N/A	
Digital certificates (hosted yes/no)	N/A	
Multifactor authentication	Yes	
Biometrics	Yes	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	No	
Branch/Point of Sale	No	
Call Centre	Yes	
Other	For more information contact the company	
Issuing process (if applicable)		
Assurance levels conformity	O Auth 2	
Online issuing process (incl lead time in working days)	Real-time digital onboarding and proofing of digital identities supporting several identity credentials - liveness checks and image recognition of global ID documents	

Face-to-face issuing (incl lead time in working days)	N/A
Issuing network	For more information contact the company
Attributes offered	
Persons	Address, age, passport
Companies	For more information contact the company
Reference data connectivity	
Connectivity to governmental data	For more information contact the company
Other databases	Background checking against more than 1,000 global watchlists
Certification	
Type	For more information contact the company
Regulation	KYC, AML, PSD2, GDPR
Other quality programs	FIDO Alliance
Other remarks	World Economic Forum Panelist
Clients	
Main clients / references	Global banks, utilities, telcos
Future developments	Zero Knowledge Proof high-assurance verification against authoritative sources

Company	Sift Science	View company profile in online database
	Sift Science is a machine learning company that fuels business growth by empowering world-leading online businesses to drive risk-free user experiences. Sift dynamically prevents fraud and abuse by combining industry leading technology and expertise, a global data network and long-term customer partnership. Global brands such as Twitter, Airbnb, Yelp!, Shutterstock, Jet.com, Indeed and Wayfair rely on the Sift Science Digital Trust Platform for access to a global network of fraud data, more than 16,000 fraud signals, and its unique ability to detect and prevent fraud in real time.	
Website	www.siftscience.com	
Keywords for online profile	fraud prevention, account takeover, content abuse, fraud detection, machine learning, ecommerce fraud, fraud prevention software, chargebacks	
Business model	SaaS	
Target market	Ecommerce, financial institutions, payment services providers, online communities, web merchants, gaming and gambling, travel, on-demand services, online ticketing, marketplaces	
Contact	sales@siftscience.com	
Geographical presence	Global	
Active since	2011	
Service provider type	SaaS technology vendor, web fraud detection company	
Member of industry associations and or initiatives	Merchant Risk Council	
Services		
Unique selling points	Real-time machine learning, global network, advanced automation	
Core services	A suite of products that prevent payment fraud, account takeover, content abuse, fake accounts, and promo abuse	
Pricing Model	Pay as you go with volume discounts based on transaction volume	
Fraud prevention partners	Soon	
Other services	Account management, integration support	
Third party connection	Contact us for more information	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	No	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	No	
Credit Rating	No	
Follow up action	Yes	
Other	Yes	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call centre	No
other	No
Reference data connectivity	
Connectivity to governmental data	No
Other databases	Multiple
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	Information Security (SOC 2 Type 2)
Regulation	N/A
Other quality programmes	Contact us for more information
Other remarks	Contact us for more information
Clients	
Main clients / references	Airbnb, Twitter, Wayfair, Yelp!, Jet.com, Remitly, OpenTable, Indeed, Zoosk, Instacart, Everlane, Patreon
Future developments	Expanding products and markets

sift science

One sophisticated platform prevents all fraud and abuse

Whether you're wrestling with fake listings, malicious content, counterfeit goods, or scams, Sift Science can help.

Our machine learning and natural language processing technology is designed to detect bad actors of all types - before they strike.

PATREON

"Sift Science is my one-stop shop. I don't have to look at anything else for useful, actionable data."

Maritza Dominguez
Trust & Safety at Patreon

Thousands of sites and applications are protected by Sift Science

match ChowNow yelp MERCARI

Company	Simility, a PayPal Service	View company profile in online database
	Simility offers real-time risk and fraud decisioning solutions to protect global businesses. Simility's offerings are underpinned by the Adaptive Decisioning Platform, built with a data-first approach to deliver continuous risk assurance. By combining artificial intelligence (AI) and big data analytics, Simility helps businesses orchestrate complex decisions to reduce friction, improve trust, and solve complex fraud problems. Built by industry veterans, Similty is trusted by some of the world's leading consumer brands across financial services, payment processors and commerce merchants. Simility was recently acquired by PayPal, and will leverge their partnership to continue developing innovative fraud and risk management solutions for the digital-first economy.	
Website	https://simility.com/	
Keywords for online profile	fraud detection, identity assurance, risk management, decision orchestration, fraud prevention, trust and safety, authentication	
Business model	SaaS and on-premise models	
Target market	- ecommerce, marketplaces, digital commerce, on-demand/sharing economy, classifieds, financial institutions, fintech (banks, mobile wallets, and more) - payment services providers (acquirers, payment gateways, payment processors)	
Contact	contact@simility.com	
Geographical presence	Global coverage with offices in Palo Alto (US), Dallas (US), Hyderabad (India), London (UK), Amsterdam (NL), and Sao Paulo (Brazil)	
Active since	2014	
Service provider type	- technology vendor - web fraud detection company	
Member of industry associations and/or initiatives	Merchant Risk Council, SOC2 Type II compliant, PCI compliant	
Services		
Unique selling points	Complete enterprise fraud management platform, with ingress processing, Device Recon, third party validation, analytics, machine learning, and case management	
Core services	Fraud and risk management	
Pricing model	Per-transaction and on-premise license pricing models	
Fraud prevention partners	Assertiva	
Other services	Data-Science-as-a-Service, historical data analysis	
Third party connection	Simility can connect to various 3rd party feeds, including internal customer data feeds.	
Technology: anti-fraud detection tools available		
Address verifications services	Yes, through third-party services	
CNP transactions	Yes	
Card Verification Value (CVV)	More information available upon request	
Bin lookup	Yes	
Geo-location checks	Yes	
Device fingerprint	Yes	
Payer authentication	Yes	
Velocity rules – Purchase limit rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit rating	No	
Follow up action	Yes	
Other	IP blacklists, device fingerprint	

Authentication context	
Online	Yes
Mobile	Yes
ATM	More information available upon request
POS	Yes
Call centre	More information available upon request
Other	Branch banking data
Reference data connectivity	
Connectivity to governmental data	More information available upon request
Other databases	Yes, we work with a variety of third party services
Fraud management system type	
Single-channel fraud prevention system	More information available upon request
Multi-channel fraud prevention system	Yes
Certification	
Type	SOC2 Type I and II, PCI compliance
Regulation	More information available upon request
Other quality programmes	More information available upon request
Other remarks	More information available upon request
Clients	
Main clients / references	Customers include Global 500 in financial services, ecommerce, payments, classifieds. Public references include US Bank, Chime, Jumia, OfferUp, Luisaviaroma, Zions Bank.
Future developments	Further interactive data visualisation and out-of-the box integrations with new data sources.


Transforming the way
analysts detect fraud
Tailored, end-to-end solutions that provide real-time fraud intelligence
Purpose-built Data Lake
Big-data Enabled
State-of-the-art, White-box Machine Learning
Continuous Rules Optimization
Powerful Decision Engine
GET STARTED TODAY
An AI-based fraud prevention and risk management platform that continuously adapts as fraud evolves. See for yourself:
WWW.SIMILITY.COM/DEMO
similityA PayPal Service

Company	ThreatMetrix a LexisNexis Risk Solutions Company View company profile in online database
	ThreatMetrix, A LexisNexis Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into hundreds of millions of anonymised digital identities, ThreatMetrix ID delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time.
Website	www.threatmetrix.com
Keywords for online profile	digital identity, authentication, identity verification, fraud detection, mobile fraud, web fraud, forensics, threat detection
Business model	Software-as-a-Service (SaaS)
Target market	- banking and brokerage - ecommerce - gaming - government - healthcare - insurance - lending - media - payment processing - telecommunications - travel
Contact	Courtney Austin, Senior Director EMEA Marketing, ThreatMetrix
Geographical presence	Worldwide: more than 185 countries
Active since	2005
Service provider type	- digital identity service provider - technology vendor - web fraud detection company
Member of industry associations and or initiatives	FIDO, One World Identity, MRC
Services	
Unique selling points	Comprehensive platform to manage fraud, authentication, and identity decisions. By seamlessly combining digital identity intelligence from ThreatMetrix with vast offline data sources from LexisNexis Risk Solutions, organisations get unparalleled visibility into the true identity of their users in order to instantly differentiate between trusted consumers and fraudsters.
Core services	Digital identity, risk-based authentication, fraud prevention, mobile security, knowledge-based authentication
Pricing Model	Tiered pricing based on transaction volume
Fraud prevention partners	ACI, Cardinal Commerce, CyberSource, First Data, FIS, Fujisoft, Gemalto, LexisNexis, nets, Paysafe and Worldpay.
Other services	Prevention against account takeover, new account registration and payment fraud; strong authentication; behavioural analytics and machine learning; bot and remote access trojan detection; professional services
Third party connection	Yes
Technology: anti-fraud detection tools available	
Address verifications services	Yes
CNP transactions	Yes
Card Verification Value (CVV)	No
Bin lookup	No
Geo-location Checks	Yes
Device Fingerprint	Yes

Payer Authentication	Yes
Velocity Rules – Purchase Limit Rules	Yes
White list/black list database:	Yes
KYC – Know Your Customer	Yes
Credit Rating	No
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities
Other	Carrier ID for strong mobile authentication
Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call center	Yes
other	No
Reference Data connectivity	
Connectivity to governmental data	Yes
Other databases	ThreatMetrix Digital Identity Network is one of the largest databases for monitoring customers providing global shared intelligence. Every day millions of consumer events are logged as well as thousands of high risk flags.
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	SOC-2 expected in 2019
Regulation	No
Other quality programs	No
Other remarks	No
Clients	
Main clients / references	Netflix, Lloyds Banking Group, Visa, Yandex.Money, Gumtree
Future developments	Continued platform integrations between ThreatMetrix and LexisNexis Risk Solutions

ThreatMetrix
A LexisNexis® Risk Solutions Company

www.threatmetrix.com

The Decision Engine for Seamless Digital Business

Fighting fraud with digital identity intelligence from billions of transactions and a powerful decision platform.

ThreatMetrix® Digital Identity Network®

Harness the power of global shared intelligence from the largest network of its kind.

40b	165k	4.5b	.8b	1.5b	185
annual network transactions	websites & apps supported	unique devices identified	unique email addresses	mobile devices	countries served globally

Company	Trulioo	View company profile in online database
	Trulioo is a global identity and business verification company that provides secure access to reliable, independent, trusted data sources to instantly verify customers and merchants online. Trulioo's instant online verification platform, GlobalGateway, helps organisations comply with AML and KYC requirements by automating due diligence workflows across borders through a single solution.	
Website	www.trulioo.com	
Keywords for online profile	regtech, KYC, Know Your Customer, AML compliance, identity verficiation, ultimate beneficial owners, identity checks, customer due diligence	
Business model	Transaction-based	
Target market	Financial services providers, banks, payments, remittance, ecommerce, gaming, and online marketplaces	
Contact	media@trulioo.com	
Geographical presence	Global	
Active since	2011	
Service provider type	Digital Identity Service Providers	
Member of industry associations and initiatives	More information available upon request	
Services		
Unique selling points	Trulioo's GlobalGateway offers clients with secure access to 5 billion people, more than 100 countries, 250 million companies, and 400 data sources through a single API integration for instant verification.	
Core services	Digital electronic identity verification	
Pricing Model	Pricing is per transaction and based on volume and complexity.	
Fraud prevention partners		
Other services	Offers Mobile ID, business verification and ID document verification.	
Offering: authentication technology used		
PIN	No	
Password/phrase	Yes (for API)	
Token	No	
Card	No	
Digital certificates (hosted yes/no)	No	
Multifactor authentication	Yes (in the portal)	
Biometrics	Yes	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	No	
Branch/Point of Sale	Yes	
Call Centre	Yes	
Other	N/A	
Attributes offered		
Persons	First, middle and last name, DOB; minimum age, gender, address, mobile/telephone number, email addres, driver licence number and expiry, National IDs	
Companies	Date of incorporation, jurisdiction of incorporation, shareholder list document, financial information document, address, mobile/telephone number, email address	

Reference data connectivity	
Connectivity to governmental data	Citizens register, company register, IDs
Other databases	Utility bills, mobile network operators, social data, credit databases
Certification	
Type	ISO27001
Regulation	KYC, AML, 4AMLD, PSD2, FCA, Fintrac, MiFID II, GDPR and FinCEN, AUSTRAC
Other quality programs	N/A
Other remarks	N/A
Clients	
Main clients / references	Trulioo is a trusted verification provider for more than 500 companies, including some of the world's top payments, ecommerce and financial services providers.
Future developments	N/A

Fraud Prevention Begins with Knowing Your Customer

Trulioo's AML/KYC solution automates the CDD process for over 5 billion people & 250 million corporate entities in 100+ countries

Accelerate your KYC process from weeks to minutes with award-winning identity verification.

Trulioo
Building Trust Online

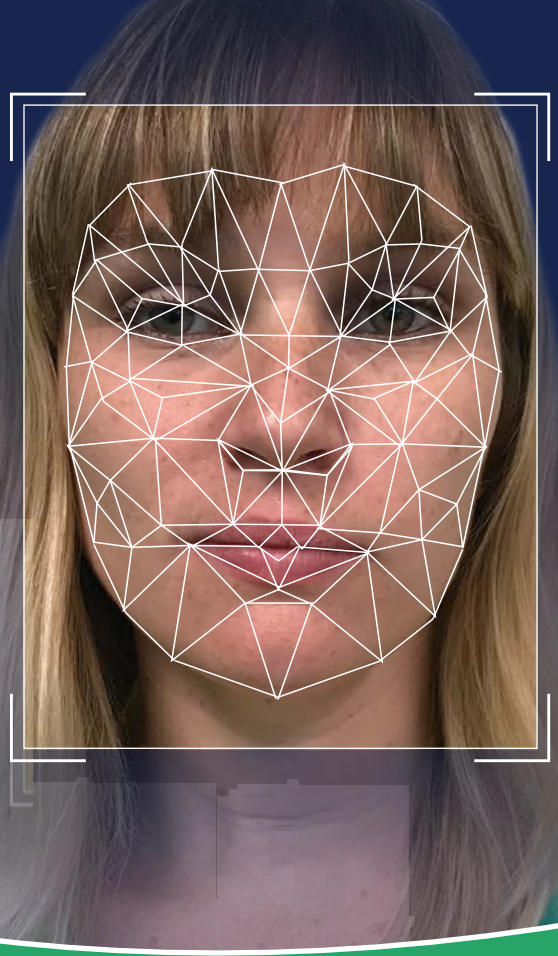
Chat with us at trulioo.com

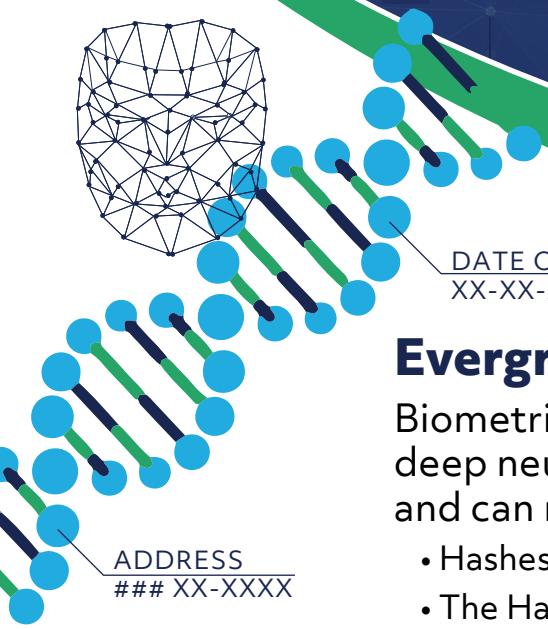
Company	Trust Stamp	View company profile in online database
	Trust Stamp provides a proprietary AI-powered hashed biometric identity solution. A one-way process converts biometric data into a hash that cannot be reconstructed into the original biometric, avoiding the security risks and legal complications of storing and transmitting PII data. These hashes solve problems like synthetic identity fraud and KYC.	
Website	https://truststamp.ai/	
Keywords for online profile	fraud, risk, protect, loss, biometrics, detection	
Business model	Per use licenses or custom product development	
Target market (limited list of markets)	Financial institutions, payment services providers, government services, P2P platforms, gaming and gambling, other online businesses, and real estate	
Contact	andrew.gowasack@emergenttech.com	
Geographical presence	Europe, North America, Latin America, Middle East & Africa	
Active since	2015	
Service provider type	Digital identity service provider, technology vendor, web fraud detection company	
Member of industry associations and initiatives	Conference of Western Attorney Generals, Biometrics Institute	
Services		
Unique selling points	Trust Stamp is a multi-factor biometric platform with inbuilt de-duplication that can be augmented with social media and other data mining or even self-warrantied identities. A unique factor is a shareable non-PII hash that tokenizes the identity and can embed both encrypted data and pivot points to external data.	
Core services	Trust Stamp uses proprietary facial biometric AI with proof of life to create tokenized identity hashes.	
Pricing	Pricing is per transaction and based on volume and complexity	
Partners	Plug and Play, The National Association of Realtors, Mastercard Startpath, QC Fintech, SixThirty Cyber, and Gerogia Institute of Technology Advanced Technology Development Center	
Other services	For more information contact the company	
Offering: authentication technology used		
PIN	Yes	
Password/phrase	Yes	
Token	Yes	
Card	For more information contact the company	
Digital certificates (hosted yes/no)	For more information contact the company	
Multifactor authentication	Yes	
Biometrics	Yes	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	For more information contact the company	
Branch/Point of Sale	Yes	
Call Centre	Yes	
Other	For more information contact the company	
Reference data connectivity		
Connectivity to governmental data	For our safety apps we search public data sources, such as criminal databases and sexual offender lists.	
Other databases	For our real estate solution we are using proprietary non-FCRA data to qualify leads for real estate.	

Certification	
Type	For more information contact the company
Regulation	KYC, PII, GDPR
Other quality programs	For more information contact the company
Other remarks	For more information contact the company
Clients	
Main clients / references	Synchrony Financial, Conference of Western Attorny Generals, Mastercard Startpath Program, Plug and Play ADGM
Future developments	For more information contact the company

TrustStamp™

Artificial Intelligence Powered Federated Trust and Identity





Evergreen Hash™

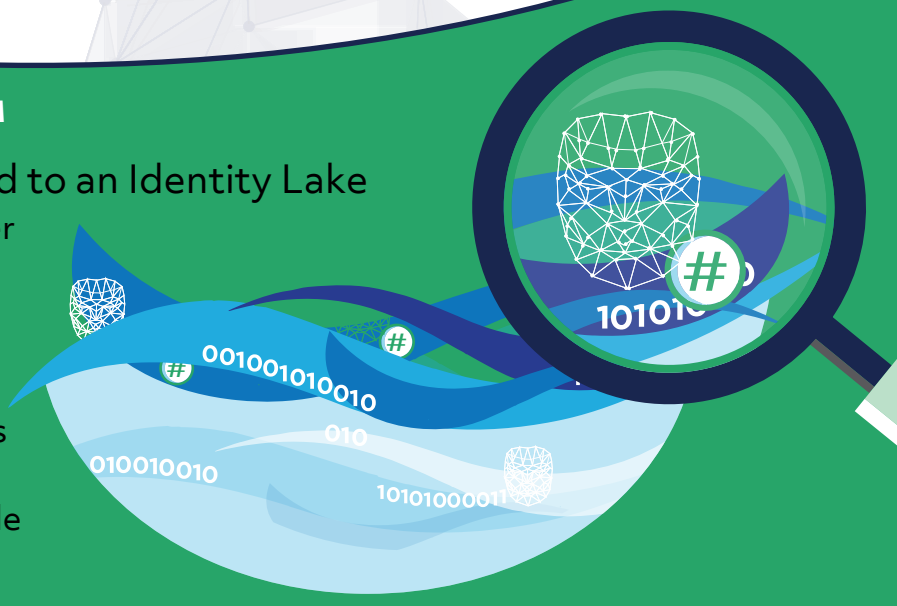
Biometric data is transformed into a 512 byte-hash using a deep neural network. The hash is pseudo-anonymized data and can never be reverse engineered.

- Hashes can be generated from any biometric data
- The Hash also offers 1.28 Bn. unique hash or encrypted data points
- Fields can contain substantive data or serve as a pivot point to external data

Hashed Identity Lake™

Once created, the hash is added to an Identity Lake

- The lake can be hosted on a server or a blockchain
- Proprietary AI predicts the probability that two hashes came from the same face, flagging fraudsters with multiple identities
- The lake can act as a non-PII data sharing consotrium with adjustable access based on agreement



Learn More at www.truststamp.ai

Company	Web Shield Limited	View company profile in online database
	Founded by highly-motivated, technology-affine professionals from the credit card and IT industries, we at Web Shield use our expertise in large-scale project management, system architecture design, software development and several investigation areas to perform risk assessments and persistent monitoring of legal entities.	
Website	www.webshield.com	
Keywords for online profile	on-boarding, underwriting, monitoring	
Business model	On-demand and subscription service	
Target market	- acquiring banks - payment service providers - financial institutions - online communities/web merchants - credit bureaus (qualitative data approach) - gaming and gambling - law enforcement - detective agencies - other online businesses	
Contact	compliance@webshield.com	
Geographical presence	Leipzig, Warsaw, London	
Active since	2011	
Service provider type	- SaaS vendor - training - consulting services	
Member of industry associations and or initiatives	Merchant Acquirers' Comittee, European Financial Coalition, Internet Watch Foundation, Electronic Transactions Association, International RegTech Association	
Services		
Unique selling points	Web Shield helps acquiring banks, payment processors and other actors in the payments space to protect themselves from bad actors involved in illegal or non-compliant activities. Our highly precise on-boarding and monitoring tools enable underwriters to make informed decisions about prospective clients, and alert them when existing ones behave dubiously.	
Core services	On-boarding and monitoring solutions	
Pricing Model	For more information please contact compliance@webshield.com	
Fraud prevention partners	Wołoszański & Partners Law Firm	
Other services	- training seminars for risk management, underwriting best practices and online investigation - regulatory monitoring, a dynamic international database with legal opinions concerning cryptocurrency regulation - organising the RiskConnect Networking Conference for Risk Professionals in Frankfurt a.M. (https://www.riskconnect.eu/) - content violation detection for Cyberlockers	
Third party connection	CreditSafe, LexisNexis, iSignthis, Vendorcom, Minera, RiskSkill, 4Stop	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	No	
Card Verification Value (CVV)	No	
Bin lookup	No	
Geo-location Checks	Yes	
Device Fingerprint	No	
Payer Authentication	No	
Velocity Rules – Purchase Limit Rules	No	
White list/black list database	Yes	

KYC – Know Your Customer	Yes
Credit Rating	Yes
Follow up action	For more information please contact compliance@webshield.com
Other	For more information please contact compliance@webshield.com
Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call centre	No
other	For more information please contact compliance@webshield.com
Reference data connectivity	
Connectivity to governmental data	Yes
Other databases	Commercial attribute providers, e.g. credit databases
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	For more information please contact compliance@webshield.com
Regulation	For more information please contact compliance@webshield.com
Other quality programmes	Mastercard Merchant Monitoring Service Provider
Other remarks	For more information please contact compliance@webshield.com
Clients	
Main clients / references	Wirecard Bank AG, Worldline SA, Concardis
Future developments	For more information please contact compliance@webshield.com

Company	Wibmo Inc. View company profile in online database
	Wibmo Inc. a Cupertino, California company is a leading provider of payment security and mobile payments in emerging markets with a leading market presence in India, one of the world's largest digital payment markets.
Website	www.wibmo.co
Keywords for online profile	Online fraud prevention, mobile app security, mobile banking, online banking, CNP fraud prevention, out-of-band authentication, multi-factor authentication, push-based authentication, EMV® 3-D Secure, behavioural biometrics, artificial intelligence
Business model	Software-as-a-Service (SaaS)
Target market	Banks, issuers, ecommerce/merchants, acquirers/PSPs, fintech, mobile commerce and mobile payment consumers
Contact	sales@wibmo.com
Geographical presence	India, Middle East, Africa, Asia, Southeast Asia
Active since	1999
Service provider type	Web fraud detection company / payment service provider (PSP)
Member of industry associations and or initiatives	Visa, Mastercard authorised processor EMVCo Business and Technical Associate PCI-DSS 3.2 certified EMVCo 3DS certified
Services	
Unique selling points	Trident the next generation intelligent enterprise fraud mitigation system performs real-time fraud detection with a combination of rules-based approach and advanced analytics powered by artificial intelligence. 1. Enterprise screening 2. Multi-factor fraud detection techniques 3. Advanced Analytics 4. Realtime Transaction Monitoring and Case Management 5. Dynamic addition of new data types and data streams 6. Realtime rules activation resulting in ability to react to fraud trends in real time
Core services	Multi-channel support - POS, ATM, ecommerce, Prepaid, and more. Case management, static and dynamic rules based engine, real-time analytics, machine learning models
Pricing Model	Varies by service model, data dimensions, volume and complexity of fraud management framework deployed
Fraud prevention partners	For more information contact the company
Other services	Fraud data network, device intelligence, account take over, identity validations, bot detections, prevention of promotional abuse, seamless authentication
Third party connection	For more information contact the company
Technology: anti-fraud detection tools available	
Address verifications services	No
CNP transactions	Yes
Card Verification Value (CVV)	N/A
Bin lookup	Yes
Geo-location Checks	Yes
Device Fingerprint	Yes
Payer Authentication	Yes
Velocity Rules – Purchase Limit Rules	Yes
White list/black list database:	Yes
KYC – Know Your Customer	No
Credit Rating	Yes

Follow up action	Yes
Other	Behavioural analytics, trident score, spend and fraud patterns, multi-factor fraud detection techniques
Authentication Context	
Online	Yes
Mobile	Yes
ATM	Yes
POS	Yes
Call centre	Yes
other	NetBanking, Prepaid, Non-Financial Systems
Reference Data connectivity	
Connectivity to governmental data	No
Other databases	Yes
Fraud management system type	
Single-channel fraud prevention system	N/A
Multi-channel fraud prevention system	Yes
Certification	
Type	For more information contact the company
Regulation	AML
Other quality programmes	For more information contact the company
Other remarks	For more information contact the company
Clients	
Main clients / references	Leading banks across Asia. More information available upon request.
Future developments	More information available upon request

wibmo

STAY AHEAD OF DIGITAL PAYMENT FRAUD!

Meet the next generation of fraud fighting system – **Trident**™. Today, the battle against fraud is 24x7. **Trident**™ helps you stay ahead of fraud and fraud trends with its real-time, dynamic, multi-channel, intelligent data analysis and fraud prevention engine. Built to EMVCo specification, **Trident**™ **RBA** is 3-D Secure 2.0 ready.

Is your authentication intelligent enough?

- MULTI-FACTOR AUTHENTICATION
- MULTI-CHANNEL DATA SUPPORT
- DYNAMIC DATA TYPE FRAMEWORK
- INTELLIGENT RISK ANALYTICS

For product demo & further queries, mail us at: **sales@wibmo.com**

Glossary

Glossary

A

Abuse list

Intelligence-sharing mechanisms used to widely disseminate tactical fraud intelligence like mule accounts, phishing sites, malware distribution sites, compromised websites, botnet IP addresses, compromised point-of-sale terminals, etc. Abuse lists may be private (available on subscription or as part of a larger fraud detection solution) or public.

Account takeover (ATO)

A form of identity theft where a criminal gains complete control of a consumer's account, such as obtaining the PIN or changing the statement mailing address and/or making unauthorised transactions.

Adaptive decisioning

A system which draws insights from multiple data sources and is armed with the agility to make real-time adjustments for maximum impact on fraud levels whilst minimising customer friction.

Address Verification System (AVS)

A service used to check the billing address of the credit card provided by the user with the address on file at the credit card company. AVS is widely supported by Visa, Mastercard, and American Express in the US, Canada and the UK.

Anti-Money Laundering (AML)

A set of procedures, laws or regulations designed to stop the practice of generating income through illegal actions. In most cases, money launderers hide their actions through a series of steps that make it look like money coming from illegal or unethical sources was earned legitimately.

Artificial Intelligence

The simulation of the processes of human intelligence by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using the rules to reach approximate or definite conclusions), and self-correction.

Authentication

A security measure that determines whether someone or something is, in fact, who or what it declares to be. An authentication process implies the verification of a cardholder with the issuing bank. Authentication often precedes authorisation (although they may often seem to be combined). The two terms are often used synonymously but they imply two different processes.

Authentication factor

A piece of information and process used to authenticate or verify the identity of an entity based on one or more of the following:

- Possession, e.g. device signature, passport, hardware device containing a credential, private key;
- Knowledge, e.g. password, PIN;
- Inherence, e.g. biometric characteristic;
- Context, e.g. behaviour pattern, geo-location.

Authorisation

Verifying that the entity initiating a transaction is entitled to perform that action.

B

Behaviour patterns

Behavioural pattern detection technologies identify fraud by monitoring the user session to detect suspicious activities or patterns. These anomalies manifest in a couple of ways:

- Transactional: The user is performing transactions that are out-of-pattern compared with normal behaviour.
- Navigational: The manner in which the user is navigating the website is inconsistent with his or her usual pattern, is inconsistent with the pattern of his or her peer group, or is indicative of the navigational pattern of a bot.

Many (though not all) transactional anomaly detection solutions require extensive data integration. Navigational anomaly detection tends to be a more lightweight deployment.

Glossary

Big Data

Large data sets that may be analysed computationally to reveal patterns, trends, and associations relating to human behaviour and interactions. By developing predictive models based on both historical and real-time data, companies can identify suspected fraudulent claims in the early stages.

Botnet

A network of computers that fraudsters have corrupted with hidden software to secretly send spam.

Bring your own authentication (BYOA)

A computing concept in which an employee-owned device, such as a key fob or smartphone, can be used to provide authentication credentials within a business environment.

C

Card capture device

A device inserted into an ATM card slot which captures the data contained on the card.

Card testing

Occurs when a fraudster uses a merchant's website to 'test' stolen credit card information to determine if the card is valid. Fraudsters can purchase lists of credit card numbers online on the 'Dark Web' at a low cost but often do not know if the cards they are purchasing are active. To test these cards, fraudsters often use automated bots and scripts to run many of these numbers through a merchant's checkout page. If a transaction is approved, the fraudster knows that the card is valid and can make fraudulent high-value purchases elsewhere.

Card-on-file (CoF)

Authorised storage of a consumer's payment credentials by a merchant, PSP, or WSP, that allows the consumer to conveniently make repeat or automatic purchases without the need to re-enter payment credentials each time.

Cardholder-not-present (CNP) fraud

Using stolen cards or card details and personal information, a fraudster purchases goods or services remotely – online, by telephone or by mail order.

Case management

In the context of fraud management, it refers to the actions required to contain and remediate the impact of a detected fraud incident. Case management system refers to the ICT tooling used to automate routine follow-up activities and facilitate case management workflows.

CCV

A unique check value encoded on the magnetic stripe and replicated in the chip of a card or the magnetic stripe of a Visa card to validate card information during the authorisation process.

CCV2 (CID)

Also known as Card Validation Code or Value, or Card Security Code. This is a unique 3-digit check value generated using a secure cryptographic process that is indent-printed on the back of a Visa card or provided to a virtual account holder.

Change of address fraud

Occurs when the fraudster obtains details of a genuine customer's account and then contacts the business to announce that he has changed address. This is usually accompanied or followed by a request for items of value such as a chequebook, debit card or statement of account to be sent to the fake new address. A false change of address is used to facilitate previous address fraud and account/facility takeover fraud.

Chargeback management

An additional service for management of claims initiated on the issuing side.

Consumer authentication

The term used to describe tools intended to verify that the person making the transaction is actually the person authorised to do so, both in-person and card-not-present transactions.

Glossary

Credit card fraud

Fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying or to obtain unauthorised funds from an account. Credit card fraud is also an adjunct to identity theft.

Credit check

From researching the customer's financial history, the vendor can make a decision regarding onboarding the user.

Compliance check

One can also check an organisation that provides PII or other data to see if that organisation is compliant with current regulations regarding data security and potential breaches.

Customer due diligence

Identification and verification of customers and beneficial owners.

Cryptography

Protecting information or hiding its meaning by converting it into a secret code before sending it out over a public network.

D

Data ingestion

The process of accessing and importing data for immediate use or storage in a database. Connected to Data ingestion is the concept of Stateless data ingestion and augmentation, which is the system's ability to ingest all types of data, structured, unstructured, from third parties and users, as well as to include device/behavioural biometrics.

Fraudsters use the dark web, the portion of the Internet that can be browsed anonymously, to search for stolen identities and credit/debit card numbers to buy hacking tutorials or other malicious services.

Deep learning

Deep learning is an aspect of artificial intelligence (AI) that is concerned with emulating the learning approach that human beings use to gain certain types of knowledge. At its simplest, deep learning can be thought of as a way to automate predictive analytics.

Delivery and returns fraud

Return fraud is the act of defrauding a retail store via the return process. There are various ways in which this crime is committed. For example, the offender may return stolen goods to secure cash or steal receipts or receipt tape to enable a falsified return, or to use somebody else's receipt to try to return an item picked up from a store shelf. Return abuse is a form of 'friendly fraud' where someone purchases products without intending to keep them.

Derived identification

Relying on the identification that took place at another instance, for example, a bank or governmental institution. Making use of derived identification also has its constraints. Next to that, it becomes less valuable if everyone makes use of derived identification. It also implies the prospect already needed to have an account at another bank.

Device fingerprinting

Device fingerprinting is a process by which a fingerprint of a connected device – desktop, tablet, smartphone, game console, etc – is captured when visiting a website.

Device identity

Device identity technology examines a combination of identifiable hardware and software attributes associated with a computer or mobile device. The unique fingerprint associated with each device can be used to recognise devices associated with fraudulent activity as well as for ongoing recognition of devices with trusted reputations. The technology is completely transparent to end users, so it does not insert any friction into the customer experience.

The mobile browser environment can be challenging to fingerprint, since there are fewer parameters to track than in the desktop browser environment. Mobile apps are just the opposite: Digital identity vendors provide software development kits to dive deep into the device and create a footprint around parameter changes (e.g. the number of contacts, the number of songs in playlists, the apps on the device) as well as create behavioural analytics around the ways in which those parameters change.

Glossary

Device location

Device location uses the sensors native to a device to identify its location. The technology is transparent to the end user and is a reliable risk indicator, particularly when used in conjunction with other layers of protection. Mobile geolocation can be very useful for payment authorisation: If a device with the issuer's mobile app is in close proximity to a payment card transaction, this can be a valuable indicator to help prevent false declines.

Device malware

With the steep trajectory of malware creation and deployment by organised crime rings, many banks have deployed technology to detect malware as well as whether a device is jailbroken or has a rootkit installed. One important consideration as businesses implement this technology is the fact that not all malware is created equal; some malware doesn't truly risk compromising the online or mobile banking session. For one type of malware, a company may choose to take no action; for another, it may call the customer; and for a third strain, it may want to shut down transactional capability immediately.

Device-user interaction

Observations of how the user interacts with the input device, e.g. the smartphone, mouse, or keyboard. Fraudsters have been known to make use of either remote-access tools within malware or misuse of legitimate remote-access software to gain control of a victim's device.

Denial of service attack (DoS)

An attack on a computer system or network that causes a loss of service to users. A network of computers is used to bombard and overwhelm another network of computers with the intention of causing the server to 'crash'. A Distributed Denial of Service (DDoS) attack relies on brute force by using attacks from multiple computers. These attacks can be used to extort money from the businesses targeted.

Digital identity

It is a collection of identity attributes, an identity in an electronic form (e.g. electronic identity).

Digital signature

A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.

Document capture

These solutions use the camera on the device to capture a picture of an identity document (eg a driver's license or utility bill), verify the credential, and parse the data into an onboarding system or ecommerce shopping cart form, minimizing the need for consumers to go through the data-entry process.

E

E-ID services

Services for entity authentication and signing data.

Electronic Data Interchange (EDI)

It is an electronic communication method that provides standards for exchanging data. By adhering to the same standard, companies that use EDI can transfer data from one branch to another and even across the world.

Encryption

A method of coding data, using an algorithm, to protect it from unauthorised access. There are many types of data encryption, and they are the basis of network security.

End-to-end encryption

Uninterrupted protection of the integrity and confidentiality of transmitted data by encoding it at the start and decoding it at the end of the transaction.

Endpoint authentication

A security system that verifies the identity of a remotely connected device (and its user), such as a personal digital assistant (PDA) or laptop, before allowing access to enterprise network resources or data.

Glossary

Endpoint protection

Endpoint protection refers to a wide range of solutions for protecting and/or detecting compromise of the end-user's computing device (desktop, laptop, mobile device etc). Endpoint protection solutions, in general, use one or more of the following techniques:

- Hardening: the solution blocks or otherwise eliminates commonly exploited vulnerabilities.
- Monitoring/Detection: the solution monitors the system and/or user behaviour and detects anomalies.
- Sandbox: the solution redirects any untrusted content to a sandbox environment that enables safe identification of malicious content.
- Anti-Virus solutions are an example of endpoint solutions that generally use a signature/rule-based approach.
- Sensitive Information Protection solutions rely more on information classification and heuristics or machine learning-based algorithms for detection of abnormal information flows.
- Malware Protection solutions rely on a combination of one or more of the three techniques.

EMV

EMV (Europay-Mastercard-Visa) is a global standard for credit and debit cards based on chip card technology. The EMV cards make in-person transactions more secure, but increase the threat of fraud in card-not-present transactions because the chip is not involved in the transaction and provides no benefit when the card is not present.

F

False front merchants

Entities who hide the true nature of their businesses and sales of card-brand prohibited goods and services. These companies do not actually engage in selling what they claim during the merchant underwriting process, and usually are involved in illicit, illegal endeavours.

False positive

It occurs when a good transaction or order is rejected by either the issuer or the merchant, due to suspected fraud.

FIDO (Fast ID Online)

A set of technology-agnostic security specifications for strong authentication. FIDO is developed by the FIDO Alliance, a non-profit organisation formed in 2012.

Fraud apps

These are fraudulent apps that work in two ways:

- simulated ad interactions;
- intentionally misleading buttons or layouts.

In the simulated ad interactions, bots trigger ad activity. With the misleading buttons or layouts, developers create layouts that overlap ads with content so users will unintentionally click the ads. Users usually have no intention of clicking some of these ads but do so because the ads are so small that they tap them by mistake. Furthermore, these types of apps can contain more ads than they are usually allowed by their operating system to serve, or display ads outside of the screen view of an application.

Fraud detection

Tools and techniques used to detect 'acts of fraud'. It includes tools and techniques for: data analysis, data mining, rule-based detection systems, supervised machine learning systems, and unsupervised machine learning systems.

Fraud management

Organisational processes to prevent, detect, contain and remedy fraud.

Fraud prevention

Processes, tools, and techniques used to prevent 'acts of fraud'. It includes communication and awareness, authentication, and other business processes controls.

Fraud screening

A checking system that identifies potentially fraudulent transactions. Fraud screening helps reduce fraudulent credit card transactions, eliminating the need for manual reviews, minimizing bad sales and improving a company's bottom line.

Glossary

Federated identity

A federated identity is the means of linking a person's electronic identity and attributes stored across multiple distinct identity management systems. Without federated identity, users are forced to manage different credentials for every site they use.

Related to federated identity is single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or even organisations. SSO is a subset of federated identity management, as it relates only to authentication and is understood on the level of technical interoperability and it would not be possible without some sort of federation.

Fingerprint recognition

The biometric modality that uses the physical structure of the user's fingerprint for recognition. In most of fingerprint recognition processes, the biometric samples are compressed in minutiae points that reduce the size of data and accelerate the process.

Fraud score

A fraud score may be available during transaction authorisation. This is a number, usually between 0 and 1,000 that represents the overall fraud risk of a particular transaction. The higher the number, the riskier the transaction.

Friendly fraud

When a consumer (or someone with access to a credit card) makes a purchase and then initiates a chargeback, saying they did not make the purchase and/or did not receive the goods or services.

G

Geo Location Detection

Set of diverse and ideally automated tests that help fraud protection solutions assess the risk of fraud involved in a specific order passing through a merchant's website. These tests might include IP to Zip Code, IP to Billing Address, High IP Cross Referencing, IP Geo Location & Proxy Detection, and NPA NXX Area Code Web Service.

Global Address Verification Directories

This feature enables fraud protection solutions to compare the address introduced by the visitor with the existing address, detecting any fake data. It also helps e-merchants keep their customers easily reachable.

Guaranteed Fraud Prevention

A kind of insurance that transfers the impact of fraud losses from the insured entity (bank or processor or merchant) to a third party. This may be linked to the implementation of specific fraud prevention solutions.

H

Hash function

A function that can be used to map digital data of arbitrary size to digital data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. With Bitcoin, a cryptographic hash function takes input data of any size and transforms it into a compact string.

Host Card Emulation (HCE)

On-device technology that permits a phone to perform card emulation on an NFC-enabled device. With HCE, critical payment credentials are stored in a secure shared repository (the issuer data centre or private cloud) rather than on the phone. Limited use credentials are delivered to the phone in advance to enable contactless transactions to take place.

Hybrid detection system

Fraud detection system that uses both rule-based and machine learning techniques.

I

Identity of Things (IDoT)

An area of endeavour that involves assigning unique identifiers (UID) with associated metadata to devices and objects (things), enabling them to connect and communicate effectively with other entities over the internet.

Glossary

Identity Service Provider

An identity provider (IdP) is a system entity that creates, maintains, and manages identity information for principals while providing authentication services to relying on party applications within a federation or distributed network.

It usually offers user authentication as a service. Relying party applications, such as web applications, outsource the user authentication step to a trusted identity provider. Such a relying party application is said to be federated, that is, it consumes federated identity.

An identity provider is considered a trusted provider that enables consumers to use single sign-on (SSO) to access other websites. SSO enhances usability by reducing password fatigue. It also provides better security by decreasing the potential attack surface.

Identity spoofing

Using a stolen identity, credit card or compromised username / password combination to attempt fraud or account takeover. Typically, identity spoofing is detected based on high velocity of identity usage for a given device, detecting the same device accessing multiple unrelated user accounts or unusual identity linkages and usage.

Identity theft

Identity theft happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit identity fraud. Identity theft can take place whether the fraud victim is alive or deceased.

Identity verification

Checking the provided information about the identity with previously corroborated information and its binding to the entity.

Identity and Access Management (IAM)

The security and business discipline that enables the right individuals to access the right resources at the right time and for the right reasons. It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

Information sharing network

In the context of fraud management, refers to a public or private service provider of one or more Abuse Lists.

InfoSec (information security)

The practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Integrator (Systems Integrator)

An entity that specialises in bringing together component subsystems into a whole and ensuring that those subsystems function together.

Intelligence

The gathering, assessment and dissemination of information that is valuable for fraud prevention and/or detection. Fraud intelligence can be strategic (activities of threat actors, etc) and/or tactical (mule accounts, phishing sites, botnet IPs, etc).

Internal fraud

Internal fraud occurs when a staff member dishonestly makes a false representation, or wrongfully fails to disclose information, or abuses a position of trust for personal gain, or causes loss to others. Internal fraud can range from compromising customer or payroll data to inflating expenses to straightforward theft. Sometimes it's an unplanned, opportunistic attack purely for personal financial gain, but sometimes it's linked to a serious and organised criminal network or even terrorist financing.

Internet of Things (IoT)

The network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other internet-enabled devices and systems.

Interoperability

A situation in which payment instruments belonging to a given scheme may be used in other countries and in systems installed by other schemes. Interoperability requires technical compatibility between systems, but can only take effect where commercial agreements have been concluded between the schemes concerned.

Glossary

Investment fraud

Investment fraud is any scheme or deception relating to investments that affect a person or company. Investment fraud includes:

- illegal insider trading
- fraudulent manipulation of the Stock Market
- prime bank investment schemes.

K

Knowledge-Based Authentication

KBA is a method of authentication which seeks to prove the identity of someone accessing a service, such as a financial institution or website. As the name suggests, KBA requires the knowledge of private information of the individual to prove that the person providing the identity information is the owner of the identity. There are two types of KBA: 'static KBA', which is based on a pre-agreed set of 'shared secrets'; and 'dynamic KBA', which is based on questions generated from a wider base of personal information.

Know Your Customer (KYC)

The term refers to due diligence activities that financial institutions and other regulated companies must perform to ascertain relevant information from their clients for the purpose of doing business with them. Know your customer policies are becoming increasingly important globally to prevent identity theft, financial fraud, money laundering and terrorist financing.

L

Level of Assurance (LoA)

Degree of confidence reached in the authentication process that the entity is what it claims to be or is expected to be.

Liability shift

The liability for chargebacks resulting from fraudulent transactions moves from the merchant to the issuing bank when the merchant has authenticated the transaction using any of the 3-D Secure protocols. Without Consumer Authentication, merchants are liable for chargebacks.

M

Machine Learning System

Machine learning fraud detection systems use artificial intelligence solutions to detect 'acts of fraud'. These techniques fall under two main categories:

- Supervised learning systems – these systems require training data sets to learn and use techniques like neural networks, bayesian models, regression models, statistical models, or a combination.
- Unsupervised learning systems – these systems are able to identify potential fraud based on techniques like clustering, peer group analysis, breakpoint analysis, profiling or a combination.

Mail Order – Telephone Order (MOTO)

MOTO accounts are required when more than 30% of credit cards cannot be physically swiped. Merchants that have a MOTO merchant account usually process credit card payments by entering the credit card information directly into a terminal that contains a keypad, by using terminal software installed on a personal computer, or by using a 'virtual' terminal that allows the merchant to use a normal web browser to process transactions on a payment service provider's website.

Malware

A software specifically designed to disrupt or damage a computer system.

Man-in-the-browser

A form of internet threat related to man-in-the-middle (MITM); it is a proxy Trojan that infects a web browser by taking the advantage of vulnerabilities in browser security to modify web pages or transaction content or to insert additional transactions, all in a completely covert fashion invisible to both the user and host web application. A proxy Trojan is a virus which hijacks and turns the host computer into a proxy server, part of a botnet, from which an attacker can stage anonymous activities and attacks.

Glossary

Man-in-the-middle

In cryptography and computer security, it is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Manual review

A technique in which merchants use staff members to perform manual checks on orders to determine which orders are fraudulent.

Merchant account

A type of bank account that allows businesses to accept payments in multiple ways, typically debit or credit cards. A merchant account is established under an agreement between an acceptor and a merchant acquiring bank for the settlement of payment card transactions.

Money laundering

The process of concealing the source of money obtained by illicit means. The methods by which money may be laundered are varied and can range in sophistication. Many regulatory and governmental authorities quote estimates each year for the amount of money laundered, either worldwide or within their national economy.

Multi-factor authentication

An approach to security authentication, which requires that the user of a system provide more than one form of verification in order to prove their identity and gain access to the system. Multi-factor authentication takes advantage of a combination of several factors of authentication; three major factors include verification by something a user knows (such as a password), something the user has (such as a smart card or a security token), and something the user is (such as the use of biometrics).

O

One-time Password (OTP)

A password that can be used only once, usually randomly generated by special software.

Open Authorisation (OAuth)

An open standard for token-based authentication and authorisation on the Internet. It allows an end user's account information to be used by third-party services, such as Facebook, without exposing the user's password. OAuth acts as an intermediary on behalf of the end user, providing the service with an access token that authorises specific account information to be shared. The process for obtaining the token is called a flow.

OpenID

An open standard that describes how users can be authenticated in a decentralised manner, eliminating the need for services to provide their own ad hoc systems and allowing users to consolidate their digital identities. Users may create accounts with their preferred OpenID identity providers, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication.

Orchestration hub

Orchestration hub is part of a fraud prevention platform that allows companies to request and receive data from third-party providers, with static, data-based identification, endpoint profiling, entity relationship, and behaviour analytics.

On-premise Solutions

A software that is installed and runs on computers on the organisation's premises (in the building), rather than remotely, such as a server farm or cloud.

Out-of-band Authentication

Out-of-band Authentication (OOBA) uses a communication mechanism that is not directly associated with the device being used to access the banking application or ecommerce site in order to facilitate a second mode of communication.

P

Passive authentication

A method where the user signs in through a Web form displayed by the identity provider and the user is requested to log in.

Glossary

Payment Application Data Security Standard (PA DSS)

PA DSS is a system designed by the Payment Card Industry Security Standards Council and adopted worldwide. It was implemented in an effort to provide the definitive data standard for software vendors that develop payment applications. The standard aims to prevent developed payment applications for third parties from storing prohibited secure data including magnetic stripe, CVV2, or PIN. In that process, the standard also dictates that software vendors develop payment applications that are compliant with the Payment Card Industry Data Security Standards (PCI DSS).

Payment Card Industry Data Security Standard (PCI-DSS)

A proprietary information security standard for organisations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) or by a firm-specific Internal Security Assessor (ISA) that creates a Report on Compliance (ROC) for organisations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

Personally identifiable information (PII) validation

Personally identifiable information (PII) is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context (eg address, email, passport number, date of birth, etc).

Pharming

A type of online fraud where people are redirected from a real website to a website impersonating a real one, with malicious intent.

Phishing

A method which allows criminals to gain access to sensitive information (like usernames or passwords). It is a method of social engineering. Very often, phishing is done by electronic mail. This mail appears to come from a bank or other service provider. It usually says that because of some change in the system, the users need to re-enter their usernames/passwords to confirm them. The emails usually have a link to a page similar to the one of the real bank.

Public Key Infrastructure (PKI)

The infrastructure needed to support the use of Digital Certificates. It includes Registration Authorities, Certificate Authorities, relying parties, servers, PKCS and OCSP protocols, validation services, revocation lists. Uses include secure e-mail, file transfer, document management services, remote access, web-based transactions, services, non-repudiation, wireless networks and virtual private networks, corporate networks, encryption, and ecommerce.

Point-to-point encryption (P2PE)

A point-to-point encryption (P2PE) solution is provided by a third party solution provider and is a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe or dip) until the data reaches the solution provider's secure decryption environment.

A PCI P2PE solution must include all of the following:

- Secure encryption of payment card data at the point-of-interaction (POI)
- P2PE-validated application(s) at the point-of-interaction
- Secure management of encryption and decryption devices
- Management of the decryption environment and all decrypted account data

Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage.

Glossary

Privacy

Privacy is the ability of a person to control the availability of personal information and exposure of himself or herself. It is related to being able to function in society anonymously (including pseudonymous or blind credential identification).

Proofing

Identity proofing is a common term used to describe the act of verifying a person's identity, as in verifying the 'proof of an ID'. Other terms that describe this process include identity verification and identity vetting.

R

Ransomware

Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment.

Real-time risk management

A process which allows risk associated with payments between payment system participants to be managed immediately and continuously.

Relying Party (RP)

A website or application that wants to verify the end-user's identifier. Other terms for this entity include 'service provider' or the now obsolete 'consumer'.

Retail loss prevention

A set of practices employed by retail companies to reduce and deter losses from theft and fraud, colloquially known as 'shrink reduction'.

Risk assessment

The process of studying the vulnerabilities, threats, and likelihood of attacks on a computer system or network.

Risk-Based Authentication (RBA)

Risk-Based Authentication is where issuing banks apply varying levels of stringency to authentication processes, based on the likelihood that access to a given system could result in it being compromised.

As the level of risk increases, the authentication process becomes more intense.

Rule-based fraud detection

Rule-based fraud detection systems use correlation, statistics, and logical comparison of data to identify potential 'acts of fraud' based on insights gained from previous (known) fraud incidents. They generally use traditional methods of data analysis and require complex and time-consuming investigations that deal with different domains of knowledge like financial, economics, business practices and behaviour. Fraud often consists of many instances or incidents involving repeated transgressions using the same method. Fraud instances can be similar in content and appearance, but usually are not identical. Rule-based systems rely on identifying a known fraud pattern.

S

Smart card

An access card that contains encoded information used to identify the user.

Secure element

A tamper-proof Smart Card chip capable to embed smart card-grade applications with the required level of security and features. In the NFC architecture, the secure element will embed contactless and NFC-related applications, and is connected to the NFC chip acting as the contactless front end. The secure element could be integrated into various form factors: SIM cards, embedded in the handset or SD Card.

Glossary

Security protocol

A sequence of operations that ensure the protection of data. Used with a communications protocol, it provides secure delivery of data between two parties.

Security threat and risk assessment

A method that identifies general business and security risks aiming to determine the adequacy of security controls with the service and mitigating those risks.

Security token (authentication token)

It is a small hardware device that the owner carries to authorise access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob.

Sensitive data

Information that relates to contact information, identification cards and numbers, birth date, social insurance number and other data that can be used for malicious purposes by cybercriminals.

SIM Cloning

A victim's SIM card data, containing all of their phone's data, is copied to a fraudster's SIM so that the fraudster can impersonate them and access all incoming communication, as well as mobile banking. To keep personal information secure, users are advised to make sure they download the latest banking apps directly from the official websites, and be wary of using financial institution contact details from SMSes or emails, as well as confirming account details via email, SMS, or telephone. Also, if a user realises (s)he is not receiving calls or text notifications, (s)he may have fallen victim to a SIM card cloning scam.

Single point of purchase

The ability to detect whether a consumer's card may have been compromised when an institution is experiencing a high volume of fraudulent transactions.

Smishing (SMS phishing)

A variant of phishing email scams that utilises SMS systems instead of sending fake text messages.

Signing (confirmation by customer)

Confirming a financial or non-financial transaction by verifying an entity's identity in a manner that is non-repudiable (i.e. using one or more authenticators).

Skimming

Card skimming is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam. In biometrics and ID, it could be the act of obtaining data from an unknowing end user who is not willing to submit the sample at that time.

Social media analytics

Social media analytics combine public and private data sources with an analysis of the consumer's social media presence. For example, an applicant who is in her mid-thirties but has no public record data nor any trace of social media presence is one who bears further scrutiny.

This type of analysis is also helpful for thin-file consumers who can't be readily verified by traditional data sources.

Spoofs

Various scams in which fraudsters attempt to gather personal information directly from unaware individuals. The methods could include letters, telephone calls, canvassing, websites, e-mails or street surveys.

Strong Customer Authentication (SCA)

In accordance with EBA Consultation Paper, the authentication procedure shall result in the generation of an authentication code that is accepted only once by the payment services provider each time that the payer, making use of the authentication code, accesses its payment account online, initiates an electronic transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

Suspicious transaction reports (STR)

A report compiled by the regulated private sector (most commonly banks and financial institutions) about financial flows they have detected that could be related to money laundering or terrorist financing.

Glossary

Synthetic ID fraud

This type of fraud occurs when a fictitious identity is created, usually with a combination of real and fake information, and is used to obtain credit, make purchases and open accounts.

T

Threat

A threat consists of an adverse action performed by a threat agent on an asset. Examples of threats are:

- a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential files from a company network or from card;
- a computer malware seriously degrading the performance of a wide-area network;
- a system administrator violating user privacy;
- someone on the internet listening confidential electronic communication.

Third-party fraud

Fraud committed against an individual by an unrelated or unknown third-party.

Token

Any hardware or software that contains credentials related to a user's attributes. Tokens may take any form, ranging from a digital data set to smart cards or mobile phones. Tokens can be used for both data/entity authentication (authentication tokens) and authorisation purposes (authorisation tokens).

Tokenization

The process of substituting sensitive data with an easily reversible benign substitute. In the payment card industry, tokenization is one means of protecting sensitive cardholder PII in order to comply with industry standards and government regulations. The technology is meant to prevent the theft of the credit card information in storage.

Transaction Authentication Number (TAN)

A type of single-use password used for an online banking transaction in conjunction with a standard ID and password.

Triangulation fraud

Considered as one of the most complex ecommerce attack methods, triangulation fraud involves three points.

- An unsuspecting customer who places an order on an auction or marketplace using some form of credit, debit, or PayPal tender.
- A fraudulent seller who receives the order and then places the order for the actual product with a legitimate ecommerce website using a stolen credit card.
- A legitimate ecommerce website that processes the criminal's order.

Trust

The firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context.

Trusted framework

A certification program that enables a party who accepts a digital identity credential (called the relying party) to trust the identity, security and privacy policies of the party who issues the credential (called the identity service provider) and vice versa.

Trusted third-party

An entity trusted by multiple other entities within a specific context and which is alien to their internal relationship.

Two-Factor Authentication (2FA)

Two-Factor Authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorised, such as a security code.

U

Unique identity

A set of identifiers/attributes forms a unique identity. Furthermore, an identifier, such as a unique number or any set of attributes, is capable of determining precisely who or what the entity is.

URL spoofing

This is an attempt to closely mimic the URL of another website. This makes the fraudulent website appear legitimate.

Glossary

User data verification

One of the first actions FIs take when onboarding a prospective new customer is verifying the individual's identifying information by comparing the data provided by the prospective customer to third-party sources. While many countries' anti-money laundering requirements mandate the verification of specific PII elements, such as name, address, and taxpayer identification number, many issuers verify more than just the bare minimum dictated by compliance. While ecommerce merchants verify PII less frequently due to cost constraints, many incorporate elements of digital identity verification into their risk protocols.

V

Verified by Visa

Verified by Visa provides merchants, acquirers and issuers with cardholder authentication on ecommerce transactions, by leveraging the 3-D Secure protocols. It helps to reduce ecommerce fraud by ensuring that the transaction is being initiated by the rightful owner of the Visa account. This gives merchants, acquirers, issuers and consumers greater protection on ecommerce transactions.

Vishing

The act of using the telephone in an attempt to scam the user into providing private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking (s)he will profit.

Voice authorisation

An approval response that is obtained through interactive communication between an issuer and an acquirer, their authorising processors or stand-in processing or through telephone, facsimile or telex communications.

Voice over IP (VoIP, or voice over Internet Protocol)

Refers to the communication protocols, technologies, methodologies and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the internet. Other terms commonly associated with VoIP are IP telephony, internet telephony, voice over broadband (VoBB), broadband telephony, IP communications and broadband phone.

W

Wire fraud

A financial fraud involving the use of telecommunications or information technology.

3-D Secure 2.0

3-D Secure (3DS) is the program jointly developed by Visa and Mastercard to combat online credit card fraud. To reflect current and future market requirements, the payments industry recognised the need to create a new 3-D Secure (3DS) specification that would support app-based authentication and integration with digital wallets, as well as traditional browser-based ecommerce transactions. This led to the development of EMV 3-D Secure – Protocol and Core Functions Specification v2.0.0 (EMV 3DS 2.0 Specification). The specification takes into account these new payment channels and supports the delivery of industry leading security, performance and user experience.

THE PAYPERS

Don’t Miss the Opportunity of Being Part of Large-Scale Payments Industry Overviews

Once a year, The Paypers releases four large-scale industry overviews covering the latest trends, developments, disruptive innovations and challenges that define the global online/mobile payments, e-invoicing, B2B payments, ecommerce and web fraud prevention & digital identity space. Industry consultants, policy makers, service providers, merchants from all over the world share their views and expertise on different key topics within the industry. Listings and advertorial options are also part of the Guides for the purpose of ensuring effective company exposure at a global level.

B2B Fintech: Payments, Supply Chain Finance & E-invoicing

Payment Methods Report

Open Banking Report

Payments and Commerce Market Guide

For the latest edition, please check the Reports section