# ECOMMERCE FRAUD TRENDS 2021

***12 of the leading eCommerce fraud prevention and payment solutions share what you need to prepare for in the coming year.***

www.merchantfraudjournal.com

# Table of Contents

# Fraudsters Will Not Make It Any Easier on Merchants in 2021

Ecommerce fraud continues to rise, and fraudsters continue to innovate new ways to defraud honest merchants. This includes new strategies like synthetic identity fraud as well as new tactics like SIM card swaps. Meanwhile, technology continues to advance; it's easier and easier for thieves to perfect and scale their operations. Newcomers and wannabe hackers can easily buy personal information, credentials, and credit card numbers stolen with algorithms and sold anonymously on the dark web.

That's just the chargeback fraud problem. Sophisticated hackers go straight for merchants' bank accounts with complex account takeover fraud (ATO) attacks that target SMBs and enterprise brands alike. These attacks increase in sophistication and audacity every day, making it harder for employees to detect them. FireEye, a security platform, estimates that 7/10 phishing emails are opened by the intended recipient.

Unfortunately, many merchants and companies respond to these threats incorrectly. Merchants respond to eCommerce fraud solely by trying to prevent chargebacks — even though the amount of revenue lost by declining good orders can exceed chargeback losses. Companies respond to ATO attacks either with generic tools provided by their email provider — a strategy proven to be ineffective — or by ignoring the problem all together.

# *Invaluable Insights to Protect Yourself Against eCommerce Fraud*

We put this guide together to help merchants, SMBs, and enterprise organizations do better to protect themselves effectively against threats. It consists of interviews with thirteen  of the most well-known and respected eCommerce fraud prevention solutions available today:

Chargebacks911® challenge the status quo

Kount®

FEATURE SPACE

GEOGUARD Fraud Has No Place To Hide

clearsale

identiq

riskified

Nethone

SEON

SIGNIFYD

T1 Payments

vesta

We asked these experts a series of questions about how merchants can protect themselves. Participation was entirely free; Merchant Fraud Journal did not receive a single penny from any solution for their inclusion. We simply reached out to solutions we know are at the forefront of today's emerging fraud prevention technologies. They did not disappoint us. They answered our call with valuable insight on a number of topics, including:

- Chargeback prevention
- ATO Fraud
- Preventing False Positive Declines
- Emerging fraudster methodologies
- Machine Learning and Data Analytics
- Fraud prevention best practices

Merchant Fraud Journal's mission is to foster collaboration between fraud prevention experts, and then pass that knowledge on to merchants. We are confident that you, our community of readers, will find this guide to be a valuable resource for improving your own understanding and practice of eCommerce fraud prevention.

Sincerely,
Bradley Chalupski - Editor-in-chief
&
Dan Moshkovich - CEO

# Chargebacks911

**Founded in 2011, Chargebacks911 is the first global company fully dedicated to mitigating charge-back risk and eliminating chargeback fraud. As industry-leading innovators, the company is credited with developing the most effective strategies for helping businesses maximize revenue and reduce loss in a variety of industries and sectors within the payments space.**

**It provides comprehensive and highly scalable solutions for chargeback compliance, handling services and fraud strategy management. The company helps decrease the negative impact of chargebacks, thereby increasing revenue retention to help ensure sustainable growth for every member of the payment channel.**

**Chargebacks911's unparalleled category experience and Intelligence Source Detection (ISD™) technology help identify the true source of chargebacks, optimizing revenue recovery opportunities, mediating disputes, safeguarding reputations, and proactively preventing future fraud.**

www.chargebacks911.com

## How will COVID-19 continue to influence eCommerce fraud prevention in 2021?

The pandemic was a tipping point for the ecommerce market. For years, it has been tantalizing consumers with its array of one-click checkouts, next day deliveries, and promise of saved time and effort. Inch by inch, it successfully drew people in from the high street to the comfort of their homes.

However, when COVID-19 struck, stores were closed and consumers across the world were effectively banished to their homes. Online shopping became more than a trend, it was (and is still) a lifeline. This inevitably drove consumer ecommerce adoption levels through the roof – with a 74% increase in online shopping. Joining it was the mass digital transformation from businesses and inexorable fraud levels.

This won't change in 2021. Even once the worst of the pandemic passes and consumers creep back towards in-store shopping, fraud will unlikely drop back to pre-pandemic levels. This is since there is more opportunity to commit fraud online, while businesses and consumers still extremely new to the sphere are targeted.

One type of fraud that has been exceptionally troublesome is account takeovers (ATOs). Attempted ATO attacks ballooned 282% between Q2 2019 and Q2 2020, with rates for ecommerce businesses selling physical goods jumping a massive 378% between March and August 2020.

ATOs must be on the radar as we head into 2021 due to reduced contact at the point of exchange, vamped up ecommerce activity, and the increased number of vulnerable businesses and customers. We would advise merchants to proactively counteract them by implementing a robust identification and verification process – not having the right security checks in place makes any merchant a prime target for fraudsters.

For the same reason, click-and-collect fraud – also known as BOPIS (buy online, pickup in store) fraud – is one to watch in 2021.

Since masses of consumers have been unable to shop in-store (or are at least avoiding it), overall BOPIS sales are expected to reach upward of $74.2 billion in the US during 2020. For fraudsters, this means increased opportunity to use stolen card details and pick up goods without needing to share a legitimate postal address, or sometimes even an ID on arrival. Research indicates there was a 55% increase in BOPIS fraud attempts in the first half of 2020 compared with the prior year, and we expect this to continue to cause trouble in 2021.

This growth in criminal fraud has also sent chargebacks on an upward spiral, since defrauded consumers are seeking to get their money back from the merchant who processed the order. That's before even mentioning the fraudulent chargebacks (friendly fraud) which have spiked this year.

Overall, the number of chargebacks being experienced by some industries increased to almost 10 times the amount taking place prior to the pandemic.

With these fraud trends expected to rise in 2021, it is crucial for businesses operating in the ecommerce industry to implement multi-layered fraud detection. There are also multiple complementary fraud detection tools they can deploy right away, including Address Verification Service (AVS), CVV verification, 3-D Secure, and geolocation. These will help nip fraud in the bud before it escalates.

**What are the trends in privacy regulation (ie. GDPR) and payments regulation (ie. PSD2) that will impact merchants and the eCommerce fraud prevention industry?**

Personal data is the world's most valuable asset, so valuable that it is vulnerable to theft or misuse. As a result, the management and use of it is under scrutiny across the globe – but the regulative response is causing many raised eyebrows.

Take the General Data Protection Regulation (GDPR), for example. While protecting consumers' personal information is a top priority, the GDPR can make it difficult to track crucial transaction data. We could end up with a situation in which merchants see new and developing risk factors, but don't have the data necessary to identify them.

Levelling up from this is India's proposed Personal Data Protection Bill (PDPB), which is reportedly on track for approval early in 2021. When in effect, PDPB as it stands will regulate how data from the country's 1.3 billion Indian residents is collected, processed, stored, used, transferred, protected, and disclosed.

PDPB uses the GDPR as a model. However, unlike the GDPR, PDPB would treat the data generated by its citizens as a national asset. This means those operating within the region will need to store and guard data from consumers in India within its national boundaries. As such, it will forbid organizations from transferring or storing sensitive personal data overseas. The Indian government would then reserve the right to use that data as a national defense and interest mechanism.

It is crucial that any business which targets Indian consumers understands what the PDPB means for them. Otherwise, as per the initial proposal, they will face penalties of up to fifteen crore rupees (approximately $2.2M USD) or four percent of the company's total gross revenue from the last financial year, whichever is higher.

In addition to this, when considering the impact of payments regulations next year, we also can't ignore PSD2's open banking. It has the potential to be one of the most significant factors to impact the payments space in 2021. Research suggests that open banking users could double between 2019 and 2021, expanding to 40 million global users. While it offers benefits for cardholders and merchants, it also creates uncertainty, which can open the door for abuse.

Now that PSD2 has begun to open the market to new players who are driving competition, there's a new directive heading our way. A major review of PSD2 will be occurring early in 2021, after which we will know more about what to expect from the much-anticipated PSD3.

**What will be the biggest 2021 eCommerce fraud trend that is currently being overlooked?**

Friendly fraud, a havoc-wreaker on the soft underbelly of merchants' operations, will continue to be overlooked as we head into 2021. While incidents have more than doubled between January and June 2020, many businesses still don't know how to spot this type of fraud, let alone prevent it.

The fact of the matter is that friendly fraud is now easier to commit than ever before. Consumers are cloaked by anonymity when shopping digitally, and contactless deliveries mean merchants are more restricted when confirming if a package arrives safely.

The moral compass of many consumers has also been hit by the unfortunate circumstances created by COVID-19. It is a sad case as consumers, worn down from the financial pressure of the pandemic, turn to filing 'item not received' chargebacks to play the system into getting a forced refund while keeping the product for themselves.

What's more, these raised levels of friendly fraud have mounted on the pressure for issuers who have been balancing a lack of staff, increased chargeback volumes, and the need to satisfy customers. As a result, the necessary diligence required for friendly fraud has been lacking, and this change in behaviour is in danger of embedding itself further.

As we head into 2021, these issues aren't likely to disappear. Following the mass digitization across many industries, it will be more important than ever for businesses to mitigate chargebacks. It will go a long way towards protecting bottom lines as merchants start to recover.

First though, they must learn how to distinguish between what is a genuine chargeback claim and what is friendly fraud. Not doing so can leave a business refunding fraudulent chargebacks, making them look like an easy target and leaving them open to repeated instances. Around 50% of cardholders who successfully commit friendly fraud will do it again within 60 days. On the other hand, merchants could end up challenging genuine disputes if the true cause of the chargeback isn't identified, which could lose them loyal customers.

To start identifying what is friendly fraud and what is not, merchants must first mend internal errors and implement solutions that tackle criminal fraud to identify and mitigate genuine disputes. This will allow them to wean instances of friendly fraud and challenge them.

Again, not challenging them can result in repeated instances, while keeping on top of them by going through the representation process shows processors and issuers that merchants mean business. Having a good reputation with everyone involved in this process will make it more likely that their cases are handled with greater care.

**Monica Eaton-Cardone**
**COO and Co-Founder,**
**Chargebacks911**

Monica Eaton-Cardone has worked for over a decade to educate merchants and financial institutions about hidden threats in the rapidly changing payment fraud landscape. Leading Chargebacks911, she established Europe's first chargeback remediation specialist to tackle the GBP 100 billion chargeback fraud problem.

Monica is passionate about the need to educate merchants and financial institutions on risks that will only get worse if left unaddressed. She was one of the earliest and most vocal voices to warn of the hidden risks of friendly fraud, including how evolving consumer behavior has caused a perpetual cycle of rising fraudulent actions.

# ClearSale

**ClearSale is an eCommerce fraud prevention solution with nearly two decades of experience, and more than 2,000 employees servicing 3,000+ brands (including enterprise retailers like Chanel, Walmart, Sony, and Rayban) around the world.**

www.clear.sale

## How will COVID-19 continue to influence ecommerce fraud prevention in 2021?

I believe that COVID-19's impact on ecommerce will still influence most of the fraud prevention trends in 2021, at least during the first part the year. It will take some time for vaccination programs to have an impact large enough for businesses to start recovering and for schools and governments to resume pre-pandemic operations. In the meantime, fraudsters will keep taking advantage of merchants and consumers wherever they can. As many retailers struggle to hold on and revive, fraud prevention will be one of the keys to their survival.

### Organized fraud will keep rising

Criminal enterprises are always ready to exploit chaos, and the move to online shopping created a shift in customer behavior that provided cover for some of their attacks. One study found that the card fraud rate increased by more than 60% in 2020 because of the pandemic, and most of that is driven by organized groups.

Account takeover fraud has increased, too, primarily by groups using stolen password files and bots to breach consumer accounts at scale. There's no reason to think that card or ATO fraud will decrease in 2021, regardless of our progress in fighting the coronavirus.

Another organized criminal tactic that's on the rise is luring out-of-work jobseekers into fraud unwittingly. The U.S. Secret Service has reported that people looking for work are being targeted by criminals to be "money mules" to launder funds. The victims take what they think is a real job and can end up in trouble with the law.

We've seen a similar phenomenon in ecommerce. International fraudsters pose as employers and hire people living in the U.S. to place ecommerce orders with data that they don't know is fake or stolen. That way the orders appear to come from a typical American consumer instead of from a location outside the U.S., so they're more likely to be approved. This type of scam is likely to persist as long as people who are desperate for work can be exploited by fraudsters.

## Individual fraud increases may persist

It's important to keep in mind that ecommerce fraud isn't just perpetrated by organized criminals. The shutdowns have also hurt individuals financially, and that has created pressure to start committing fraud. In one survey, more than a third of consumers in the UK said they'd committed friendly fraud since the start of the pandemic.

People who take this route may rationalize their behavior, saying that they're only turning to fraud because they're out of work and have no other support. They might commit friendly fraud, claiming that items they ordered never arrived, or commit return fraud by using an item and then sending it back for a refund.

Until the economy recovers, people who take this approach may feel justified in continuing to commit small-scale fraud, regardless of the damage it causes to merchants and their employees. Even after the economy recovers, people who've picked up the habit of fraud may continue if they don't see any consequences.

## Government assistance programs need stronger safeguards

Fraudsters pounced on government unemployment and small business relief funds that were rolled out in 2020. Using lists of stolen personal information and compromised passwords, organized criminals have launched account takeovers and identity theft schemes that divert relief funds from people who need them.

Scammers have also been phishing prospective unemployment applicants and other people into turning over their credentials or entering them into a site where they could be captured and used to submit false claims. In some cases, the very people who need assistance have had their applications delayed or denied because fraudsters already filed claims in their name. When the scam claims that the applicant worked for a particular company that employer can be affected, too.

Unfortunately, this is another pandemic-related problem we expect to continue into 2021, because it's still going strong now. In October, FinCEN, the U.S. treasury department's financial crimes enforcement network, released an advisory for employers and banks about five different unemployment insurance fraud schemes they're seeing more of due to the pandemic, including account takeovers and synthetic identity fraud.

All of that means that employers, financial institutions and government agencies will need to be more vigilant and proactive in 2021, as long as there are relief funds that criminals can exploit. FinCEN's advisory includes a list of scams and red flags to watch for, and California has added safeguards that make it harder for criminals to impersonate aid recipients. Any agency that administers relief funds needs to review the way they verify applicants' identities and deliver funds, so that we don't see the same level of fraud in 2021 that we saw in the early days of these programs.

## BOPIS is here to stay—and so are the fraud prevention challenges

BOPIS (buy online pick up in store) has been increasing since the start of the pandemic—by June 2020, nearly 70% of American consumers were using BOPIS—and lots of people will keep their BOPIS habit in the year ahead.

Fraudsters have capitalized on this trend, and fraud rates in this channel rose 250% over the previous year, according to Merchant Fraud Journal's BOPIS Retail Trends report. And while BOPIS relies on CNP transactions, its risk profile for fraud differs from a standard online order.

For example, there's no shipping address to compare to the customer's billing address or to a list of known fraud-related addresses. For BOPIS orders with quick pickup—for example, restaurant curbside orders—there's not a lot of time to analyze orders that raise fraud flags. And, as the MFJ report noted, slow communication between order systems and store staff can allow fraudsters to cancel orders just before pickup and then claim the goods anyway.

To reduce BOPIS fraud in the year ahead, merchants need to improve data visibility, so staff know as soon as an order is canceled. Merchants also need the capacity to quickly manually review orders that raise any flags.

## Old-fashioned CNP transactions require extra fraud detection

Call center and MOTO transactions have increased since pandemic shutdowns took hold, as grocers, restaurants and other local businesses work to serve customers who may not have internet access or who aren't comfortable ordering online.

MOTO is important for expanding consumer options. But it's a riskier channel in terms of fraud because telephone and mail orders don't give us access to some of the strongest variables that we normally have to predict fraud, like device fingerprint and the user's behavior on the website.

Fraudsters know this, of course, and that puts merchants at risk for MOTO-related chargebacks. That's why card brands like Visa urge merchants to take extra precautions with phone orders they suspect may be fraudulent, like asking for extra contact information and in some cases extra time to verify the transaction.

Taking those steps requires merchants to train their customer-facing employees to do this in a friendly, professional tone. It also puts the burden on employees to recognize MOTO fraud flags, many of which align with pandemic-era good customer behavior, like a first-time shopper placing a larger than normal order. Because MOTO chargeback liability falls more heavily on merchants than the card issuer, merchants with a high or growing percentage of MOTO transactions should consider working with a third-party fraud prevention service in the year ahead to protect their revenue.

**What are the trends in privacy regulation (ie. GDPR) and payments regulation (ie. PSD2) that will impact merchants and the eCommerce fraud prevention industry?**

The 2021 deadlines for implementing PSD2 and its secure customer authentication (SCA) requirements in Europe will impact some of the largest markets in the world. SCA's two-factor authentication is designed to help curb the massive growth in card-not-present fraud in the UK and Europe. Reducing fraud is a good thing, of course, but it's clear that the market is apprehensive about the potential impacts of SCA, such as more friction during checkout, more declined orders and more customer abandonment.

However, there's no consensus yet on how SCA may affect ecommerce sales. Because most merchants have postponed implementation of SCA in their stores, there's limited transaction data to study. Microsoft has been testing SCA in Europe for more than a year now and reporting their results each month on LinkedIn. As of October 2020, their data showed that app-based authentication is performing poorly on most key indicators. A high number of customers are asked to provide additional information, and those challenges lead to increases in checkout abandonment. Two bright spots in Microsoft's reports are that the time required to complete a challenge has dropped below one minute, on average, and that successful challenges lead to more approvals

Based on that information, it appears that SCA could influence the channels that consumers use. For example, if mobile transactions are harder to complete or more likely to be declined, shoppers might switch to computers to complete their orders or perhaps even go to the store in person. And PSD2 allows consumers to whitelist their favorite stores as "trusted beneficiaries" so they can skip providing extra authentication steps like a code or a fingerprint at checkout. But it's possible that many shoppers will simply switch to a merchant with an easier-to-use SCA implementation for mobile commerce.

The European deadlines for SCA enforcement also have the potential to cause some confusion among merchants about requirements for individual transactions, because the EU and the UK have SCA enforcement deadlines that are several months apart—Jan. 1 in the EU and Sept. 14 in the UK. Depending on where the card is issued, UK merchants could be required to apply SCA ahead of the in-country deadline for UK-issued cards. It's not clear yet how merchants will be able to do this.

Based on the data that Microsoft has collected in its SCA tests, it seems that many systems weren't ready to deliver a good customer experience with SCA as recently as October. That creates a competitive advantage for retailers who have already tested and optimized their SCA implementation, and of course it also creates a hurdle for retailers who need to catch up. We'll start to see the impacts more clearly in the EU in January. The hope is that merchants will be able to make quick improvements to their SCA processes to retain their customers and experience a reduction in fraud.

**What will be the biggest 2021 ecommerce fraud trend that is currently being overlooked?**

Open banking will bring new challenges along with benefits for financial institutions, merchants and consumers. Fintech startups are offering lots of new solutions for virtual cards, rewards programs, and mobile apps that work with existing institutions—and consumers have responded strongly. In 2020, the number of U.K. open banking customers doubled to more than 2 million, for example.

Open banking is convenient and delivers benefits like discounts and credit improvement tools. Open banking also helps banks streamline their data to operate more efficiently. However, the strength of open banking—sharing customer data—is also a potential weakness. Some of the data that gets shared will inevitably be the product of criminals using synthetic fraud, identity theft, and account takeovers to create or hijack payment and rewards accounts. In Q2 2020, account takeovers increased by more than 280% from the previous year, and there's no reason to assume that growth will stop or taper off in 2021.

Many of the attacks that target open banking can't be stopped with card fraud prevention tactics because they don't involve the direct use of a card. Instead, open banking needs an "identity fraud" approach, including new data points in traditional fraud scores, to protect consumers, merchants and banks. Developing those new safeguards will be one of 2021's challenges.

**Rafael Lourenco EVP and Partner, ClearSale**

Rafael Lourenco is Executive Vice President and Partner at ClearSale, a card-not-present fraud prevention operation that helps retailers increase sales and eliminate chargebacks before they happen. The company's proprietary technology and in-house staff of seasoned analysts provide an end-to-end outsourced fraud detection solution for online retailers to achieve industry-high approval rates while virtually eliminating false positives.

# Featurespace

**Featurespace™ is the world leader in enterprise financial crime prevention for fraud and Anti-Money Laundering. Featurespace invented Adaptive Behavioral Analytics and created the ARIC™ platform, a real-time machine learning software platform that risk scores events in more than 180 countries to prevent fraud and financial crime.**

www.featurespace.com

## Adapting to Change: Today's Fraud Detection Requires Advanced Analytics

The global pandemic has changed our personal and professional lives beyond recognition, but one of the biggest shifts in behavior has been in how we shop. With various restrictions on what stores customers can physically enter and a preference for transactions that are as contact-free as possible, the ongoing transition to a cashless society has significantly accelerated this year.

With more and more countries re-entering lockdown, a growing number of bricks and mortar merchants will move online – some for good – meaning e-commerce will become the de facto shopping experience. And it's got some big boots to fill.

This situation doesn't look like its going to disappear at the same speed with which it arrived. Accordingly, online retailers will need to continue adapting to stay competitive and satisfy the increasing consumer demand by delivering:

- Easier ways to pay: Wallets, tokenization and pay-by-bank;
- Less friction: Seamless user journeys that don't hit a brick wall when it comes to handing over their money; and
- Expanded options: Try before you buy, online purchase with in-store pick-up and subscription-based services

### Opportunity knocks

While these all afford customers more flexibility, they also provide more headaches for merchants and more avenues for fraudsters to exploit. There are many increased risks that come with greater digitization and we can expect to see a continuation of first party fraud and an increase in disputes, as well as ongoing attempts to take over accounts.

In addition, financial institutions also have to factor in the complexity of distributed teams working from home, which affects the reliability and speed of investigations, leaving a large number of claims incorrectly classified as fraudulent when they're actually legitimate purchases gone wrong.

This can have far-reaching consequences. Incorrectly classified cases are the result of machine-learning models that are not picking up what "true" fraud really looks like, which will increase false positives. By not effectively performing, the models create friction in the shopping experience, which is not satisfying if you're a customer.

## Trends in privacy regulation

2020 has seen more data breaches than ever and with an influx of new online accounts, there's a greater risk of more personal details getting compromised.

At the end of the day, who is responsible for our data? The company whose website we enter it into? The social media platform we use? Truthfully, we all are. Consumers need to protect their own personal information as much as their physical possessions because there's always someone that wants to steal it.

We control who, what, when and where we use our data, and we enter a relationship with these entities, trusting that they will only use it for its intended purpose. While that is not always the case, we should be guarded and not divulge too much information. There is nothing wrong with leaving an air of mystery about ourselves online as well as in person.

According to McKinsey, synthetic ID fraud is the fastest-growing type of financial crime in the U.S. It is claimed that more than 60% of fraud losses for large banks are a result of identity fraud and 20% of that can be attributed to synthetic identity fraud.

The European Union's General Data Protection Regulation (GDPR) is set to become the most influential data protection legislation worldwide. Some other countries have similar data privacy laws to protect peoples' data, including:

- Brazil (Lei Geral de Proteçao de Dados);
- Australia (the Privacy Amendment (Notifiable Data Breaches) to the Privacy Act);
- Japan (the Act on Protection of Personal Information); and
- South Korea (the Personal Information Protection Act).

Ultimately, more counties are expected to either join hands with international data privacy committees or for new laws within the country to keep a check on privacy issues. Add to this the increased number of new merchants who are playing catch up with the second iteration of the Payment Services Directive (PSD2) – as well as GDPR – and we can expect to see more fines being levied in future.

## The future of fraud

The fraud prevention industry isn't taking anything lightly and has been hyper-vigilant for quite some time. 2020 has been an anomaly for so many reasons and it has been impossible to predict the next twist in the tale, with people giving up trying to second guess what is coming next and putting all their efforts into protecting their customers.

The collaboration between organizations that we've seen this year must continue because we're truly all in this together. Burger King telling people to eat to McDonalds is something that nobody thought they'd see but shows a sense of awareness and respect for demand and delivery. Healthy competition isn't possible without market demand and companies have done very well in coming together to sustain economies and reinforce the greater good.

What can acquirers do to support their merchants as the payments industry rapidly shifts? First, by working closely with issuers to ensure consumers feel safe using new technologies. Unless older generations trust their devices to improve their experience and make it safe, they won't use it.

Second, it's important (and mutually beneficial) to educate merchants and offer training to conquer the fear of the unknown, understand the benefits of new technology and assist with implementation.

Third, it is vital to inform tech companies of what is needed to increase adoption. New products and solutions aren't going to get the necessary traction if the demand isn't there or people don't realise the potential benefits.

## Leading the way

The Government of Canada recently launched new measures to help small businesses access global markets during the pandemic. With international travel restricted, the support package is pivoting to help small businesses:

- Develop and expand their e-commerce presence by covering partial costs associated with online sales platforms and digital strategy consulting, as well as advertising and search engine optimization;
- Attend virtual trade shows and other industry events; and
- Navigate new COVID-19-related trade barriers by helping pay for new international market certifica-

This level of support will hopefully be implemented in other parts of the world, while also expanding to include security and risk awareness. Attention must also be paid to the strain on operational teams that are facing peak period volumes each day. Fraud analytics needs to automatically adapt to shifting trends, as rules-only engines aren't sustainable.

How we live, work, and shop has changed and has now become a new normal. It's not only individuals that need to learn to change to meet its novel demands, but the machine-learning models that decipher genuine behavior from fraud have to adapt, so as not to introduce greater friction into our lives and impact already-overrun operational teams.

With the world in a constant state of flux, what was accepted convention yesterday isn't necessarily right today and models need to be flexible and evolve. Retuning is admissible for slow-moving data sets, but not for the level of change we're seeing now. Only adaptive behavioral models can meet the demand of the ever shifting 'normal' and bring a sense of consistency to our lives.

**Steve Goddard**
**Fraud Market Expert, Featurespace**

Steve Goddard has worked within the fraud and payment industry for over 15 years, in the banking, travel and retail space. He has worked closely with merchants advising on fraud strategies as well as running operations teams. He has worked with Banks and PSPs globally in product management roles, leading major development initiatives to deliver solutions to external customers.

# GeoGuard

**At GeoGuard, we focus solely on geolocation-based security, fraud detection and the protection of digital content and assets. As the independently rated market leader for protection against VPNs and Proxies, we help a wide range of industries guard against fraud and piracy while ensuring geolocation compliance with minimal user friction. GeoGuard provides a suite of geolocation-based solutions that are combined with human intelligence in order to stop internet users from spoofing their location.**

**GeoGuard's solutions are based on the award-winning geolocation and geo-protection technologies that its parent company GeoComply developed for the highly-regulated and complex digital gaming industry. Our software is installed in over 400 million devices worldwide, putting GeoGuard in a uniquely powerful position to identify and counter both the current and newly emerging geolocation fraud threats.**

**With GeoGuard, fraud has no place to hide.**

www.geoguard.com

## How will COVID-19 continue to influence eCommerce fraud prevention in 2021?

The pandemic spurred digital transformation, particularly for brick-and-mortar merchants. In fact, 35% of merchants in the U.S. launched an online store for the first time since March 2020 [1]. Merchant acquirers and merchants rapidly onboarded a massive volume of customers during this time, overwhelming their platforms and revealing weaknesses in their existing and often manual KYC processes. Bad actors exploited cracks in the system to perpetrate fraud in the form of fraudulent merchants, account takeovers and synthetic identity fraud.

With a growing need to verify more people online, 2021 is the time for merchants, merchant acquirers and payment service providers (PSPs) to adopt the use of 21st-century technology to fight online fraud. In its Guidance on Digital Identity, the Financial Action Task Force (FATF) recognized geolocation data as a necessary part of digital identity and KYC verification [2]. Yet despite the ready availability of highly accurate location data from users, very few merchants and PSPs have upgraded their systems to process anything more useful than an easily spoofed IP address.

Adding accurate and authentic location signals as part of an online verification process gives financial entities greater certainty about a user's true digital identity. Payment service providers can reduce the number of fraudulent sub-merchants they onboard onto their platform and slash the incidence of fraud.

[1] Ware2Go, COVID-19 Brings a New Era of Logistics as Merchants Plan for 2020 Holiday Peak, September 22, 2020.

[2] Financial Action Task Force, Guidance on Digital Identity, March 2020.

**What are the trends in privacy regulation (ie. GDPR) and payments regulation (ie. PSD2) that will impact merchants and the eCommerce fraud prevention industry?**

PSD2's new Strong Customer Authentication (SCA) requirement highlights the importance of multi-factor authentication in fraud prevention. Similarly, FATF's guidance notes that the authentication process is considered more robust and trustworthy when it incorporates multiple factors. Using multiple authenticators, such as geolocation or biometric data, enables a more holistic and detailed understanding of a user's true identity in order to mitigate fraud. Geolocation data is a good approach for passive authentication, increasing acceptance rates without impacting user experience.

**What will be the biggest 2021 eCommerce fraud trend that is currently being overlooked?**

This is more of an overlooked approach to fraud prevention than a trend, but it's a vital one: sub-merchants, merchant acquirers and payment service providers don't use location data when onboarding, performing KYC or authenticating transactions. They're missing an important risk signal, since there's a direct correlation between detecting and stopping location fraud and stopping all fraud.

A recent GeoGuard survey found that 50% of U.S. consumers who share or are likely to share their location data with banks do so to help these institutions better protect their accounts from fraud. And 40% of consumers and 55% of millennials and Gen Z indicate they would switch to a bank that uses location data in order to secure their accounts.

The willingness to share location data to prevent fraud should encourage payment service providers to ask for and use this information for behavioral analysis, increasing their confidence that they are signing up legitimate sub-merchants. For even higher confidence, location checking can be employed throughout the sub-merchant's session – at log-in, when sub-merchants are updating account and banking details or at other sensitive times. Account access can also be restricted to a geofenced location for an additional level of security, to stop account takeover fraud.

**Trevor Wingert**
**KYC & Anti-Fraud Solutions, GeoGuard**

Trevor has over two decades of experience building safe, empowering online and mobile user experiences. He has designed and implemented fraud and risk management solutions for a variety of e-commerce and payments companies. These include turnkey client onboarding, customer decisioning and CIP compliance solutions for payment facilitator and point-of-sale lending companies. At GeoGuard, he is developing innovative applications built on the company's advanced geolocation security technology for the financial service, fintech, and payments markets.

# Identiq

**Identiq is a peer-to-peer identity verification network that allows companies to validate new users and vouch for ones they trust - without sharing any sensitive customer data or identifiable information whatsoever.**
**By taking third-party data providers out of the equation, Identiq leverages the consensus of other network member companies. These include some of the world's largest consumer-facing companies, collaborating to accurately fight fraud and identify trusted users.**
**Recognized by Gartner™ as a Cool Vendor for Privacy in 2020, Identiq sets a new standard for end-user privacy. At the same time, it reduces false positives, increases approval rates and creates a better user experience.**

www.identiq.com

## How will COVID-19 continue to influence eCommerce fraud prevention in 2021?

The changes we've all lived through since the start of the pandemic have been dramatic, and even once things begin to settle down again, the consequences will still be there. Many will continue to impact the fraud attacks that merchants see, and the ways fraud prevention teams must act to detect and prevent them.

There are numerous ways the pandemic has affected eCommerce fraud and fraud prevention, but I'll highlight a couple which I think have generally been overlooked amongst the wide ranging shifts of the last year or so.

### Gig Economy Fraudsters: Mules, Admin and BOPIS

Unfortunately, the economic uncertainty around the world has made it easier for fraudsters to find mules in locations across the globe, giving them more options when it comes to getting around shipping restrictions or suspicions.

It's also created a larger pool of people willing to take on the grunt work of setting up accounts, signing into them and using them to browse occasionally, making aging an account easier than ever for the more sophisticated fraudster in charge of these "gig economy" workers. This trend, again, won't be going anywhere soon.

The BOPIS trend (buy online pick up in store), which has exploded in the last year and was particularly notable over the 2020 holiday period, is also susceptible to attacks exploiting such gig economy fraudsters. The geographical aspect of BOPIS, which used to be a partial protection for merchants, has been shredded.

The challenge is for merchants to continue to find ways to provide the customer experience their users expect, to match their evolving needs - without allowing that to enable fraud.

## Refunding Fraud

This is something fraud prevention pros learned back in the economic crisis of 2008 as well: In times of uncertainty, refunds go up. Not all of those are legitimate. When they build up, they can become a serious drain on your resources.

In the time of COVID-19, this has taken on a new dimension. Professional fraudsters are now widely advertising their services to ordinary consumers, offering to carry out refund fraud on their behalf, for a small percentage fee.

The consumer gets the benefit of the fraudsters' considerable experience and expertise (some fraudsters even know the precise script a specific merchant's customer support team follow, and which agents are most susceptible to which tactics) and receives the goods at a fraction of the price.

The fraudster can operate at scale, and without having to fake information in the initial order - because that one is placed by the real consumer, and so won't show up as fraudulent. The merchant pays for it.

This type of fraud tends to go unnoticed because it happens after checkout, which many fraud teams are not responsible for protecting. Also, it's so difficult to pinpoint, since the person placing the original order really is the real customer.

As this problem grows - which it has over 2020, and which it seems set to continue doing over 2021 - merchants who have remained oblivious so far are likely to wake up to the real pain of the problem. They're also likely to look to fraud prevention teams to solve it.

Collaboration between merchants who are seeing refunding fraud is likely to be the best defense, given that standard fraud fighting methods aren't a perfect fit here. Merchants who work together using privacy enhancing computation to ensure no personal user data is ever shared can collaborate closely and directly to identify the repeating perpetrators, and add friction or blocks as necessary.

**What are the trends in privacy regulation (ie. GDPR) and payments regulation (ie. PSD2) that will impact merchants and the eCommerce fraud prevention industry?**

This is a very interesting question, and certainly one that's close to my heart. Privacy is something that's extremely important to me. I even closed down a nascent business because I didn't want to have to work with the third party data brokers who take, share and sell so much of our sensitive personal information.

In terms of privacy regulation, I think it's important to look outside the EU as well as within it. California saw CCPA go live in 2020, and passed CRPA in the November elections. A federal privacy bill in the US looks likely to come up for consideration in 2021. On top of that, there are the privacy regulations in Australia, the UK, Brazil and so forth. Privacy has become a global concern, and regulators are acting on that internationally.

There's a strong feeling that things have gone too far in terms of third party data sharing, and you can see the range of reactions trying to limit this. Thus far, fraud prevention has been an exception - meaning, companies can share data with their fraud prevention vendors - because it stops crime.

However, that's not to say that fraud prevention will be untouched by the regulations. For one thing, in the EU, teams are subject to the same requirements as other departments in terms of being able to find and work with their data, in accordance with GDPR, so that a justifiable request for access or deletion can be followed through. Other privacy regulations may well take a similar track.

Moreover, the network of third party data brokers who also assist merchants and vendors in enriching their information may not benefit from all of the same exemptions. The fight between the UK's ICO agency and Experian - and the huge fine being threatened - shows that the wider ecosystem may be affected by these changes.

Fraud prevention teams may need to consider alternative routes for enriching their understanding of their users. Here Privacy Enhancing Computation, one of Gartner's top tech trends for 2021, may be helpful, enabling companies to leverage one another's knowledge and trust in users without sharing any personal user data. This tech trend, which as Gartner notes is gathering steam, may propel the providerless trend in fraud prevention to expand its reach.

Regarding PSD2 and all the associated changes - the great tension here is between compliance and customer experience. PSD2 was originally kicked off, after all, to enable more open banking and the advantages and convenience it provides.

Different merchants, in different industries, will likely find different optimal ways of dealing with this. The more merchants work together, and with regulators, this year, the greater the chances of an optimal balance being reached all round.

## What will be the biggest 2021 eCommerce fraud trend that is currently being overlooked?

Account-level fraud! This hits from two directions - new user accounts, and ATO. Both are dangerous, in different ways, and both are currently underestimated as a threat because they aren't part of the transaction flow.

Yet even though this fraud trend isn't at the point of purchase, where most fraud prevention effort and energy usually goes, the potential damage is considerable, and very serious.

### New Users, New Challenges

The flood of new users many merchants saw in 2020 occurred as people turned online to fill the gaps left by their reduced access to offline shopping and activities. You might well think that with time, this will become less relevant, as those who were going to make the shift online will already have done so.

Yet this isn't entirely the case. Firstly, users who were new to online purchases in March and now feel themselves to be veterans might still be new to your store even in late 2021. With the enormous uptick in consumers moving online, it's likely that there will be a long-tail effect in terms of individual sites seeing new users.

Fraudsters, of course, will be well aware of this, and poised to take advantage, hiding more easily among the new shoppers. Merchants struggling to deal with the increased numbers are less likely to notice accounts being set up with fake, stolen or synthetic data. With the large numbers in play, fraudsters can also afford to set up some accounts for immediate use, and have others go through the aging process so that they look more legitimate when the time comes for them to leverage them.

Fake accounts leave your business open to a range of vulnerabilities, including fake reviews, buyer-seller collusion in marketplaces, and fundamental uncertainty about the scale and nature of your user ecosystem.

In 2021, effective fraud prevention and identity validation will need to start well before the point of purchase. Otherwise, far too much is left unprotected.

### Account Takeover in 2021

ATO is always a challenge, of course, but in 2021 it's a greater risk than ever. Back at the start of the pandemic, phishing attacks rose by a whopping 667%, and have continued to be a major attack vector ever since.

It only makes sense; fraudsters are capitalizing on a chance the likes of which they never even dreamed of. People are working from home, using domestic infrastructure that's far less secure than that of their place of work. They're stressed, and often busy dealing with both work and personal challenges - children who are now at home, or parents who are high risk. They're dealing with all kinds of new sites. They don't have the time or mental space to be as suspicious as they might be in more ideal circumstances.

Despite the increase in phishing, there hasn't been a corresponding spike in ATO attempts. There has been a rise, but not on the same scale. Which makes it likely that some fraudsters are playing a long game, planning to use this windfall of stolen data over a longer period, when merchants are less likely to be looking for it. This is likely to be at its peak over 2021, because waiting too long with the data of course leaves the risk that users may change their information.

Account takeover represents a risk at checkout, with fraudsters using the good reputation of established accounts to make their purchases look more legitimate. That process starts before checkout - since fraudsters can explore purchase history to make their order look more probable.

Additionally, there are a range of nefarious activities that can take place within the account, from stealing, adding and changing user information (including credit card and shipping address) to siphoning off credits, money or gifts through loyalty points or other such programs.  More than that, ATO is a risk in itself; 65% say they would likely stop buying from a merchant if their account was compromised. Identify verification methods need to be implemented much earlier on in the process of consumer interactions.

Fraud prevention can't afford to focus on the point of purchase in 2021. Fraudsters are coming for your accounts.

**Itay Levy**
**CEO and co-founder, Identiq**

Itay Levy is Identiq's CEO and co-founder. Prior to Identiq, Itay was the CEO and founder of Appoxee, a mobile marketing automation platform designed to increase engagement, which he successfully sold to Teradata in 2015. Before Appoxee, Itay was a part of the founding team of Buzzmetrics, a Social Media Research company acquired by Nielsen for $150M in 2006. Itay holds a BA in Computer Science and an EMBA from the Kellogg School of Management at Northwestern University.

# Kount

**Kount's award-winning AI-driven digital fraud prevention solution is used by 9,000+ brands globally, helping them to reach their digital innovation goals. Kount's patented technology combines device fingerprinting, supervised and unsupervised machine learning, a robust policy and rules engine, self-service analytics, and a web-based case-management and investigation system. Kount's solutions stop fraud and increase revenue for digital businesses, acquiring banks, and payment service providers.**

**www.kount.com**

## How will COVID-19 continue to influence e-commerce fraud prevention in 2021?

In 2020, the coronavirus pandemic changed commerce almost overnight, with dramatic changes in transaction volumes for companies engaged in eCommerce. Some businesses saw big drops, while others set records for online transactions, and others entered into eCommerce at scale for the first time. Each of these scenarios presents various risks for fraud. As businesses and consumers continue to adjust to a permanent digital shift, fraudsters will also adjust, and the impact of COVID-19 will carry forward into 2021. With factors such as economic stressors, bad actors may be more compelled to engage in fraud to make money and take advantage of companies that are not properly equipped for their digital transformation.

These factors will make more aspects of the customer journey vulnerable, even more so than they are today. Fraud occurs far beyond the point of payment, and we'll see that trend continue to evolve in 2021. Fraudsters are likely to move away from individual financial transactions or individual interactions as a whole toward larger, single effort opportunities, such as breaking into a company's customer base and accounts, taking over their accounts, and depleting them of any prepaid funds, and doing it at scale as opposed to engaging in hand-to-hand combat.

## What are the trends in privacy regulation (ie. GDPR) and payments regulation (ie. PSD2) that will impact merchants and the eCommerce fraud prevention industry?

These regulations continue to be promulgated by jurisdictions worldwide, including comparable legislative initiatives. At Kount, we realize the impact these steps have on companies engaged in digital commerce, and we closely monitor them globally on a monthly basis by country. Some countries make adequate provisions to leverage data and data assets to secure transactions and prevent fraud. However, there are ideas that do not carve out those particular uses of data, and this will make it much more difficult for the good guys to do their fraud prevention work and much easier for the bad guys to engage in fraudulent activities. Continuing into 2021, there will be a balancing act between adhering to regulations, providing an excellent customer experience, and preventing fraud. For companies engaged in global commerce, a trusted partner is key to understanding and managing the vast requirements associated with eCommerce.

**What will be the biggest 2021 e-commerce fraud trend that's currently being overlooked?**

In 2021, eCommerce companies will need to think about the entire customer journey and how to establish identity trust at any point, even more so than in previous years. In particular, accounts will be vulnerable, with a greater number of attacks at account creation, account takeover, or other vulnerabilities to commit fraud at scale. Any businesses engaged in digital commerce or digital interactions with their customers would be remiss if it hasn't addressed account protection by early 2021, or even better, late 2020.

Meanwhile, a key area many currently overlook is the opportunity to proactively use fraud insights to drive revenue. Flipping the script from fraud prevention to establishing identity trust with actionable customer insights and advanced data will be key for eCommerce businesses looking to grow and thrive. This means creating personalized experiences.

Business used to be conducted entirely face-to-face. The guys at the men's clothing and shoe stores that I go to can give me personalized recommendations because they know me; they know what's in my wardrobe. This experience of highly personalized interactions is key to success and loyal eCommerce customers.

In this new, digital-first world, anyone engaged in digital interactions, from merchants to insurance companies, is going to have to find new channels to get to know their customers to make those recommendations or understand when not to do so. This requires gaining actionable data transparent insights from their service providers and partners, such as Kount. These insights can help accelerate business growth only if it's returned to them in an actionable form. At Kount, we take the vast amounts of data that merchants create and help them leverage our artificial intelligence to recategorize that data to be useful so they can prudently grow their business.

**Brad Wiskirchen**
**CEO, Kount**

Bradley J. Wiskirchen is the founding CEO at Kount, the leading digital identity trust and fraud prevention solution. Among his many other community involvements, Wiskirchen was the Chairman of the Board of the Salt Lake City Branch of the Federal Reserve Bank of San Francisco in 2014 and 2015. He was a member of the board for three years prior to serving as the Chairman.  He has also served on the High-Level Advisory Group of the International Monetary Fund's Interdepartmental Working Group on Finance and Technology.

# Nethone

**Nethone is a Machine Learning-based fraud prevention Software-as-a-Service company that allows online merchants to holistically understand their end-users also referred to as “Know Your Users (KYU)” in industry parlance. With cutting edge Machine Learning technology, Nethone is able to detect and prevent card not present fraud, including protection against account takeover (ATO).**

www.nethone.com

## How will COVID-19 continue to influence eCommerce fraud prevention in 2021?

Due to C-19, E-Commerce is growing at an even faster pace than it was before for established players. But it will accelerate the process for traditional retailers to move towards ecommerce, and they will certainly require expanded support in fraud prevention. I think you’ll see a number of new players in eCommerce, including some companies that have been traditionally focused on brick and mortar retail. And they will need more support, and fast. You might think that during a pandemic customers would become less demanding and more forgiving of their favorite stores, but of course the reverse is true. Physical store closures and restrictions on movement means that customers immediately expect more options for shopping, paying, and receiving their purchases. New, well-funded players in eCommerce will be prime targets for online fraudsters who will try classic scam techniques.

New players means new deployments of eCommerce operations, which means more opportunities to target cloud systems for fraudsters. The most common technique as of late has been remote exploitation of cloud applications, accounting for 45% of cloud-related cybersecurity events examined in “Cloud Threat Landscape Report” by IBM. Oftentimes, vulnerable applications are present in an environment but remain undetected.

There is an example where friendly hackers turned a single dead link from a legacy cloud solution into an account take over method on EA/Origin last year. One of the important takeaways from the report about the “friendly” incident: “It is important that organizations with customer facing online portals carry out proper validation checks on the login pages they ask their users to access. They must also perform thorough and regular hygiene checks on their entire IT infrastructure to ensure they have not left outdated or unused domains online.” EA/Origin doesn’t exactly qualify as the brick and mortar stores example mentioned above, but the incident demonstrates the possibility of exploiting cloud systems, even those of seasoned professionals in eCommerce. IBM reported that threat actors take advantage of misconfigured cloud servers to siphon over 1 billion records from compromised environments in 2019. We have seen how fraudsters turn around and sell stolen information for extremely low prices in darknet markets and increasingly the Clearnet as well.

In addition to brick and mortar transformation, during COVID one could also see that the importance of online marketplaces is constantly growing and that this will be the only way for (some) stores to survive. Of course demand for Amazon's services exploded with C-19, but what is interesting is that it also sparked their competition. Good examples are players like Otto, Cdiscount and Conrad. Amazon remains the 800 pound gorilla in the room, but we can expect to see their competition to continue to grow massively as well. We can also expect that the growing online marketplaces will in turn become the new targets of online fraudsters.

Account takeover (ATO) scams were already becoming more popular before C-19 hit the world; with the growth explosion of e-commerce and online marketplaces, we can expect ATO to gain steam. Most merchants offer a customer account feature because they're effective mechanisms for repeat business. They're also easy to break into for scammers and are useful for both quick crimes and long term fraud.

Finally, payment behaviour of customers has changed and will continue to change. Credit cards, ATM cards, other payment cards, and cash will be less important and the relevance of instant bank transfer will grow in e-commerce. Of course this trend has already been in progress, but it is really crazy how the crisis made cash so unpopular so quickly. Mobile banking and payments apps add a level of security and convenience to users. And as previously mentioned, the crisis has been a boon for e-commerce transactions and put a damper on in-person transactions. Naturally, almost all e-commerce transactions are "card not present," which is a favorite target for fraudsters.

**What are the trends in privacy regulation (ie. GDPR) and payments regulation (ie. PSD2) that will impact merchants and the eCommerce fraud prevention industry?**

GDPR in Europe no longer stands alone in data privacy protection. More and more countries are enforcing new data protection laws. Most recently, Brazil's Lei Geral de Proteção de Dados (LGPD) joined the GDPR and CCPA (California Consumer Privacy Act) as the flagship data privacy regulations in the world. While improving the situation for users, this leads to more complexity for merchants and providers as one needs to make sure to comply with local rules.

LGPD already went into effect on September 18, but fines/penalties for non-compliance will not be implemented until May 2021. Fines for non-compliance with LGPD are potentially substantial, but not as high as GDPR penalties: the maximum administrative sanctions under the LGPD is 2% of the company's Brazilian revenue of up to R$50 million (EUR 11.2 million) per infraction. This is compared to 4% of global revenue or up to EUR 20 million under GDPR compliance.

The LGPD applies to any private or public individual or company with personal data processing activities that are carried out in Brazil and personal data is collected in Brazil. The LGPD aspires to be “transborder” and applies to global businesses, headquartered anywhere in the world, that meet these criteria as well, not just to businesses owned by citizens of Brazil.

Lei Geral de Protecao de Dados (LGPD) will certainly require an immense, concerted effort to implement, but the results will certainly be worth it: privacy protections for the people of Brazil, which translate into livelihood protection, and a healthier ecosystem for transacting business in the region. We recommend that you consult your legal counsel to begin the diligence process and (if necessary) LGPD implementation as soon as you can.

In regards to payments in particular, SCA and PSD2 will have a massive impact. Generally I expect a strong shift towards open banking solutions and a stronger growth of domestic card schemes at the cost of international card schemes.

It’s good to keep in mind that PSD2 is actually directed at banks, and merchants are affected downstream. This means that issuing banks that approve non-compliant transactions are the ones that will be penalized. Of course merchants should ensure that their transactions are compliant to avoid the risk of issuing banks refusing their transactions. In the near future, denial of transactions will most likely increase as all parties grow accustomed to SCA Requirements.

Merchants should focus on building a phased plan of implementation, A/B testing and iterative releases in order to ensure that the introduction of SCA causes minimal disruption to their purchase flows. I talk to merchants and payment providers every day, so I know that PSD2/SCA implementation is still and will be a challenge! I recommend getting started right away as approximately 2⁄3 of EU and EEA countries will begin to require Strong Customer Authentication at the end of Q4 2020 through Q1 2021.

**What will be the biggest 2021 eCommerce fraud trend that is currently being overlooked?**

There are too many to mention. In Brazil I consider the new PIX system as a tremendous challenge, for both providers and customers. In wide parts of Africa, mobile money is growing massively and is very sensitive to fraud due to the lack of available data attached to such payments. As far as general trends go, I expect a frictionless user experience to be the biggest challenge, especially associated with account based payments. In(direct) relation phishing attacks and ID theft will certainly increase.

Also, we have seen that merchants who sell stolen customer accounts have expanded to the Clearnet (you can find them on Twitter, Discord, etc.) and ATO techniques have gone mobile. Our company's intelligence specialists studied the ATO scam packages that are available for purchase in a couple of the top darknet markets. Many of today's account takeover packages come with helpful tutorials. What could be a big surprise to members of the anti-fraud community is that as of late, there are more tutorials for use with mobile devices than with desktop PCs.

More and more fraudsters have turned to mobiles for their action. We did a survey of the tutorials - 43% of the tutorials advise committing ATO with mobile apps. Only 31% of the tutorials contain instructions for using PC browsers for scams. 9% can work on both. In the remaining 17%, there were no instructions for what type of devices should be used. We surveyed our current clients too. They informed us that 40% of their ATO attacks come from mobile devices, which corroborates what we observed in the fraudster markets. We found that a good way to predict the upcoming trends in online scams is to read through the tutorials that come with the fraudster pastebin and software packages.

Going back to the brick and mortar shops (mentioned above), 28% of the ATO tutorials were for in-store fraud (when a fraudster has to physically go into a shop) and almost all of them were connected to accounts with reward points. 17% of the tutorials recommend using accounts to buy gift cards as it is one of the simplest ways to cash out money from an account with a linked payment method. So companies that are expanding from brick and mortar focused operations can expect to see an increase in mobile + in-store scams once stores are permitted to re-open.

Companies that are building omni-channel retail strategies on the fly can expect to be targets of scams. Omni-channel is an approach to sales and marketing that provides customers with a fully-integrated shopping experience by uniting user experiences from brick-and-mortar to mobile-browsing and everything in between.

The idea has been around for a few years, but COVID has been a force multiplier for the trend. A good example is Galeria Kaufhof Karstadt department stores in Germany which became Amazon hubs during COVID. The German department store giant and Amazon have been partners since 2017, but with COVID came a surge of demand for Amazon and other e-commerce services. So customers purchase goods online and pick them up offline.

But it also works the other way round: people are shopping in stores and expect the goods to be shipped to their home within 24 hours. It appears that the same operation is being implemented in the US, as Amazon is in talks to turn Sears and JCPenney locations into fulfillment centers. So brick and mortar shops are becoming even more "e-commercialized," if I may coin such a term. So omni-channel strategies are exciting growth opportunities, but they also open up new avenues for ATO and refunding scams.

**Patrick Drexler**
**Head of Business Development**
**Nethone**

Experienced sales and partner manager in the payment and financial industry with 10+ years of experience. Prior to joining Nethone, Patrick managed the partnership department at Paysafecard (for Europe and Asia), and later represented the group in Germany. For the last 5 years, Patrick has built up the partnership department at Dalenys/Natixis Payment in France and led the sales activities in the DACH area.

Patrick is building and executing the business development strategy for sales and partnership teams to establish an international footprint for Nethone.

# Riskified

**Riskified is the AI platform powering the eCommerce revolution.  Commerce has transformative powers, and at Riskified we believe everyone should have the opportunity to take part. We use advanced artificial intelligence to eliminate barriers to eCommerce. Our AI platform collects and analyzes eCommerce data to spot patterns that no one else sees, recognizing opportunities for increased revenue and reduced risk. We began as an eCommerce fraud-prevention solution, but our unique ability allows for much more than that. Today, in addition to preventing fraud, we protect shoppers' retail accounts, increase bank-authorization rates, improve communication between merchants and financial institutions, and provide shoppers with financing through Deco, giving everyone the chance to join the revolution. Riskified has reviewed hundreds of millions of transactions and approved billions of dollars of revenue for merchants across virtually all industries, including a number of Fortune 500 companies.**

www.riskified.com

## How will COVID-19 continue to influence e-commerce fraud prevention in 2021?

In 2021, consumers will still do more of their shopping online than ever before. Merchants, on their end, will continue their efforts to capitalize on this trend, grow their market share, and earn lifetime loyalty. During the pandemic, we saw merchants roll out special promotional offers and relax policies for account holders. For example, many airlines have lifted restrictions on money-back or miles redeposit when customers cancel their flight.

Fraudsters, of course, see a golden opportunity in merchants' growing reluctance to disappoint or anger their loyal customers. For them, this spells more lucrative account takeovers (ATO). In fact, in recent months, we saw fraudsters upgrade the classic ATO attack. In the past, breached accounts were used to purchase goods for resale (using stored or stolen payment methods). Now, fraudsters sell the accounts for profit.

How does it work? Once a fraudster obtains the victim's login details, they place an order using the payment method stored in the account. They purchase a low-risk product so as not to raise any flags, and ship the product to the victim's address. After the order is approved, the fraudster cancels it, but instead of asking for a refund, they ask for the value in store credit. Now the fraudster has a stolen account with stored credit in it, which increases its dark web market value.

For fraud management systems, ATO orders are tricky to intercept because the information matches that of the legitimate account holder. That's why the best way to prevent ATO attacks isn't to try and identify the fraud at checkout – but rather to block the fraudster's attempt to login to the account, nipping the fraud attempt in the bud. Merchants should leverage spoofing detection and analyze password entry behavior to detect bad actors at the first point of contact.

**What are the trends in privacy regulation (ie. GDPR) and payments regulation (ie. PSD2) that will impact merchants and the eCommerce fraud prevention industry?**

Governments are increasingly coming to understand that shoppers' data is valuable and that there are bad actors who want to misuse it. GDPR and PSD2 highlight the responsibility that merchants and other players in the eCommerce and online payments space have to be thoughtful and careful about how data is collected and used.

It's a tricky balance. Allowing customers to save a card on file is an excellent way for merchants to boost loyalty and make it easy for returning customers to complete their purchase. But, compromised information in the wrong hands can have a lasting impact on brand reputation. Riskified's solution gives merchants the confidence to operate in full compliance with the regulations without sacrificing revenue or customer experience.

PSD2, which strives to make payments safer and more secure and protect consumers from fraud, will also introduce new challenges to an already complex ecosystem. Once PSD2 is enforced across Europe, it will likely prevent fraud to some extent in intra-European transactions, but at a cost. And SCA is certainly not 'fraud-proof' and fraudsters are already busy finding ways around the new safeguards. Fraudsters are resourceful and adaptive. A brief skim of the Dark Web demonstrates just how astute they are at scheming to find loopholes to two-factor authentication. And with PSD2 presumably making their lives harder, they will try to exploit whatever they perceive to be the weakest link:

- Fraudsters trying to avoid SCA are likely to obtain details of cards issued outside Europe, as this will ensure the purchase is out of PSD2's scope.
- We expect to see fraudsters targeting the account login stage of the online shopping journey and performing account takeover (ATO) attacks, in an attempt to abuse or exploit merchants' rewards programs or avoid SCA by identifying as returning customers who had whitelisted this merchant at the Issuer side.
- Fraud at call centers might be on the rise, as mail and telephone (MOTO) orders are out of scope for PSD2.

While most merchants are focused on basic compliance and the more technical aspects of preparing for PSD2, it's important to consider the processes required to effectively cover those out-of-scope orders from a fraud-prevention perspective. Savvy merchants need a holistic fraud-prevention solution to ensure that they remain protected from new attack vectors and emerging threats.

**Jed Alpert**
**VP Marketing, Riskified**

Jed Alpert is a passionate senior marketer with a 20+ year track record of leading global marketing teams at B2B SaaS companies. As VP of marketing at Riskified, an AI platform that helps eCommerce merchants increase revenue and manage risk at every stage of the purchase funnel, he is responsible for developing Riskified's brand, voice, and marketing strategy.

# SEON

**At SEON, we strive to help online businesses reduce the costs, time, and challenges faced due to fraud. With a real-time, flexible API, we collect all the relevant risk-related data points, and after connecting them, we provide a risk score that leverages data enrichment and machine learning.**

www.seon.io

## How will COVID-19 continue to influence e-commerce fraud prevention in 2021?

The COVID-19 pandemic that hit the world in 2020 and the following government reactions forced changes in the economy that will have long-lasting effects in the world of eCommerce. As offline activities were shut down, economies worldwide were shaken. Many industries came to a grinding halt or are facing a recession, while consumer spending shifted in a way that accelerated the growth of eCommerce in a wide variety of sectors.

If one would name two notable actors, it would be the tremendous growth of home delivery services or the explosion of video conferencing software - both hallmarks of a wider and deeper economic transition that has been looming on the horizon for quite a while, but it took an unforeseen event to really hasten their development from occasional services to household must-haves.

It is hard to say whether or not developments like these will stick. On one hand, the headlines about more efficient vaccines against the pandemic situation promise a future in which life returns to normal. On the other, once consumer habits change, they tend to take root as people get used to the newly acquired comforts - as well as having made the appropriate changes in their daily lives, which might be harder to unwind. Furthermore, the economic fundamentals of our cities seem to be changing, as more businesses are adopting work-from-home schemes, which translate into less foot traffic in formerly busy areas, which are vital for the survival of brick and mortar businesses. In layman's terms, even if we return to "normal", this might not be the same as before, but rather a world where the gains made in eCommerce in 2020 stay to replace some of the daily business we have dealt with offline as part of our routines.

From a risk management viewpoint, this situation translates into three major developments that merchants should pay attention to:

### Those affected by the economic downturn might turn to crime as a form of supplemental income

While it's highly unlikely that most people would become cybercriminal masterminds overnight, we have been seeing a rise in what could be termed opportunistic fraud: an almost casual increase in friendly fraud, abuse of promotional programs, false claims of no delivery, etc. This means that risk management procedures should be adjusted appropriately, taking into account such possible motivations. In periods of economic anxiety, risk models are normally turned conservative, and businesses should take proactive steps in establishing trust with their clients, as opposed to the booming period prior to the pandemic, when we could afford to be laxer.

Another worrying development is the rise of what could be called "Crime as a service" industry, solutions that lower the barrier to entry for cybercrime. Similar to how no code solutions allows people with no technical skills to become online entrepreneurs, we are seeing a market spring up on delivering everything from ID proofing documents, proxies, fingerprinting dodging services, credit card details and so on. One-off fraudsters could quite conceivably become career criminals far more easily than even a few years ago.

In practical terms, risk rules should accommodate stricter spending limits that are tied to verified forms of authorization in the case of an eventual chargeback dispute, and new accounts should be monitored more closely, especially if you offer welcome bonuses - it's worth being a bit paranoid, and if your offers sound like something that could be abused by committed laymen, be prepared for the occasion.

### If consumer spending shifts, so does fraud

Professional criminals follow the money - it is easier to hide in a crowd after all. With the lockdown regulations affecting so many diverse areas of life, we have experienced with some of our partners that they have seen an increase in sophisticated fraud attacks. If we think in real-world terms, cybercriminals are professional enterprises: if their main source of income is cut off (because say, regulation steps in or the entire industry is suffering a downturn) they will quickly adapt and find new targets.

This is a huge risk for fast-growing businesses who normally operate under optimistic assumptions, and may be caught by surprise in case elaborate fraud rings target them. It is in your best interest to invest in the education of your risk management team, not just looking at your own numbers, but keeping up to date on the tactics employed by fraudsters, and pro-actively setting up detection mechanisms. While this might seem like over-investing in a problem that has yet to hit, it's in fact common sense. It's always worth having a fire extinguisher and a fire alarm, even if the house never burned down before, so to speak.

Above we mentioned that consumer habits, once changed, tend to stick. Imagine the same with a professional criminal enterprise who has discovered that your service is completely unprotected against the scheme they specialize in. Without sufficient risk checks on your transactions (especially on payouts and withdrawals), you may start bleeding money without noticing it. By the time you do catch them, they have gained an appetite, and now you have a sticky problem to deal with. Investing early on detecting advanced fraud schemes acts as a deterrent - cybercriminals also think about investing and risks-rewards, and nine times out of ten they would rather go for an easier target than trying to scale well-built defenses.

## What will be the biggest 2021 eCommerce fraud trend that is currently being overlooked?

We tend to forget that a large part of what's driving the eCommerce explosion is mundane but convenient technology. One example is the fact that by now most services offer to remember the user's credit card details, which is a huge convenience for both merchants and customers and is part of the "magical" online shopping experience.

The other is the relative ease of identity card based verification with the help of a smartphone that lets merchants onboard more customers with ease of mind, even if it means some additional costs and friction.

We take both services for granted, which means we might forget the additional risks they carry in the long run. The first example means that the average value of a user account has increased dramatically, as fraudsters don't necessarily need to acquire a person's credit card details, when they can simply leverage open-source intelligence gathering and acquire user logins on the darknet, via phishing or on darknet marketplaces to make a steal.

The abundance of identity verification checks likewise is fueling the development of criminal enterprises aimed at delivering the necessary documents to beat them. This is especially dangerous, as these checks are often considered fool-proof (and hence demand a hefty price from the service provider), and yet they are easily circumvented by approaches as mundane as simply paying someone for their ID and a selfie. Alarmingly, we have heard that criminals are attempting to use face-swapping technology as well, which may seem funny, considering the state of the consumer technology, but the rapid advance of deepfakes means that they will be deployed in serious fraud attempts. We have already seen successful CEO fraud stories with the use of synthetic voice technology, and beating image-based biometrics are the next frontier.

### Better safe than sorry

Merchants then should not just rely on the technology that delivers them convenience, but they must prepare for the downsides as well. Account takeover attacks should be proactively monitored, and KYC processes should take into account the fact that ID verification is not foolproof anymore, and further checks might be required to verify whether or not the user is in fact who they are claiming to be.

To that end, we will see fraud prevention systems rely more and more on digital footprint analysis for KYC either manually or automatically via data enrichment, as a form of low-friction verification that can give a more holistic overview of their customers.

The alternative to that would be even stricter biometrics, such as asking customers to perform live face gestures. And while we are sure that people are more than happy to adopt new habits around daily online purchases, we are less confident about how much “weirdness” verification processes can allow before leading to cart abandonment.

**Bence Jendruszak**
**Co-founder and Business Operations Manager,**
**SEON**

Bence Jendruszak is the Co-founder and Business Operations Manager of SEON. His vision is to create a safer environment for online high risk merchants. This is why together with his team has developed SEON, a unified risk management solution able to serve the needs of fraud managers.

# Signifyd

**Signifyd empowers fearless commerce by providing an end-to-end commerce protection platform that protects merchants from fraud, consumer abuse and revenue loss caused by friction in the buying experience.**

www.signifyd.com

## How will COVID-19 continue to influence e-commerce fraud prevention in 2021?

COVID-19 will have three big influences on fraud prevention in 2021 — two operational and one behavioral.

On the operational side of the equation, fraud and risk professionals will need to continue to operate as remote teams. Even with vaccines on the way, it will be months into 2021 before any country reaches a level of immunity that makes it safe to go back to something close to normal work routines. Until then, offices will need to be sparsely populated or not populated at all.

Even once offices are fully open and risk teams can literally huddle to analyze new fraud trends or to review orders that raise novel red flags, those teams will want to be prepared for another dramatic event that requires teams to scatter to their homes again. COVID-19 and 2020 have provided a lesson: Business continuity plans are no joke. They need to be practical and robust.

Not only will e-commerce fraud and risk professionals want to be ready for dramatic disruption, they will need to be prepared for high order volumes, probably close to those they've been managing throughout the pandemic. Online sales are still trending 50% higher than a year ago, according to Signifyd's Ecommerce Pulse data.

The dramatic surge in online orders might recede somewhat once the virus is vanquished, but consumers have told us they intend to stick to some of the habits they've formed during the pandemic. In fact, 49% of U.S. consumers told us in a September poll that they would be shopping more online a year from now than they were a year ago. In the UK, the figure was 57%. Not only that, 26% in the U.S. said they'd use curbside pickup more and 34% said they'd take more frequent advantage of buy online pick up in store. In the UK, 48% said they'd be using click-and-collect more a year from now than they were a year ago.

All these changes — more online orders, more click-and-collect, more curbside pickup — put a strain on fraud and risk teams. More orders mean more orders to review. More buy online pick up in the store or at the curb means a need for speed. The service loses its appeal if an order can't be ready for pickup in an hour or two. It also means the need to review orders without extremely useful signals that come with a delivery address. Pickup orders, of course, come with no delivery address.

During the pandemic, and before, frankly, we've worked with merchants to automate their order flows and to automate their fraud review. Signifyd combines big data and machine learning to sift fraudulent orders from legitimate ones instantaneously.

We've also essentially helped merchants tap into a vast network of orders coming from thousands of retailers, meaning it's likely that that BOPIS customer has been seen somewhere else on Signifyd's Commerce Network. It's the sort of assurance that makes up for not having a delivery address.

Beyond the operational changes retailers will need to embrace in 2021, comes a behavioral change on the part of consumers that is both challenging and discouraging. Signifyd polling and data indicate that consumers' sense of fair play when it comes to shopping have shifted during the months-long pandemic. The number of consumers who say they have committed friendly fraud appears to have increased since pre-pandemic days.

We see this as the biggest fraud trend that is currently being overlooked. We'll get into the whys and wherefores of this trend later in this piece.

**What are the trends in privacy regulation (ie. GDPR) and payments regulation (ie. PSD2) that will impact merchants and the eCommerce fraud prevention industry?**

If not in 2021 then soon after, businesses including retail businesses in the U.S., will be subject to their own version of the General Data Protection Regulation (GDPR) currently in force in Europe. California has already passed a version of privacy protection regulation. It's only a matter of time before other states and ultimately the federal government follow.

Privacy has become a key issue for consumers and politicians alike. Frequent data breaches have consumers concerned and rightfully so.

Given the inevitability of stronger consumer privacy protections, retailers should view privacy as a part of the customer experience they provide. Why not build stronger relationships with customers through transparency? When new transparency regulations come about, consider sharing with customers the ways in which you're meeting, and maybe exceeding, them.

Consumers have demonstrated that they are interested in the social, ethical and moral standing of the retailers and brands they do business with. Why not show them that your business appreciates the value of customers' personal information and that you're as interested in protecting it as they are?

Less speculative in nature is the impact that PSD2 and it's strong customer authentication requirement will have on European retailers and retailers selling into Europe. Enforcement in much of Europe begins Dec. 31., and the state of readiness among retailers and banks appears uncertain.

Consumers appear to be in for a surprise, too. Nearly three-quarters of UK consumers told us in a September poll that either were not aware of SCA or not sure of how SCA would affect them. That same poll, conducted by market research firm Upwave on behalf of Signifyd, indicated that 47% of consumers were somewhat or very likely to abandon a transaction that required two-factor authentication, which essentially is what SCA does.

Clearly, affected merchants need to get their SCA act together and quickly. Not to sound like a broken record, but again the wise approach is to see PSD2 and SCA as customer experience opportunities.

Besides the security requirements, PSD2 offers retailers opportunities to take more control of their payment stack. The regulation allows merchants to become payment initiation service providers, which means they can request payment directly from a shopper's bank account — with the customer's permission.

When a retailer acts as its own PISP, it not only saves fees associated with third-party payment players, it also gains access to consumer data and account information that can help retailers provide better, more personalized experiences for customers.

**What will be the biggest 2021 eCommerce fraud trend that is currently being overlooked?**

The recent rise of friendly fraud, including return fraud, has been one of retail's most surprising trends. Not so much that it's happening, but the speed with which it is growing. In our U.S.-based September poll, Signifyd found that 40% of consumers in the U.S. had falsely claimed that a legitimate charge on their credit account was in fact fraudulent in order to keep a product and receive a refund. More than one-third said that they had falsely claimed that a package they ordered online had never arrived or had arrived in unsatisfactory condition.

When we asked consumers a similar question in pre-pandemic January, only 14% indicated that they had falsely claimed that an online order never arrived or that it arrived in unsatisfactory condition. It's reasonable to assume that COVID-19 and all it's caused has something to do with the 19-percentage-point rise in less than a year.

Our best hypothesis is that the financial strain and psychological stress brought on by months of job losses and sheltering at home has knocked the moral compass of consumers out of whack for a segment of shoppers.

First, when money gets tight, people get desperate. Second, being told what you can and cannot do gets old after months on end. Some give in to the urge to rebel. And third, there is a sense of unfairness. COVID is something that's happening to us. We didn't ask for it. How about we inflict some of the misery we're feeling on what we see as a profitable retailer with plenty of money to spare?

Whatever the reasons behind the trend, it's something that fraud and risk teams are going to have to be ready for in 2021, if not now. Like so much in life, being proactive is the best way to combat friendly fraud.

First make sure the product descriptions and photos on your digital sites are detailed and accurate. When customers know what they're getting they are much less likely to be disappointed when a product arrives. Use the data you have to explore your customers buying behavior and to consider whether purchasing behavior you're seeing is an anomaly. Also consider whether you're seeing patterns you've previously seen by customers who abused your policies in the past. Obviously you want to give those orders extra scrutiny.

If you can, rely on transaction data beyond your enterprise. Without access to outside transactions, you won't be able to spot first-time customers who have abused other retailers' policies or committed friendly fraud elsewhere.

Watch for trouble signs after shipping, too. If you see incoming returns coming from a location different from the delivery address, that should raise red flags. That kind of incongruence could be the sign of a criminal ring running a return fraud scheme.

If you issue refunds once a return has been logged at the UPS or FedEx store, consider the data you receive concerning the incoming package. Is the weight significantly different from what was shipped out? You could be receiving an empty box or a box of sand, rather than that top-of-the-line camera you shipped.

Study your return policies. They should be easy to find and easy to understand. Sometimes consumers file a false claim for a refund rather than go through the trouble of hunting down your policy or parsing legalese to figure out what is and isn't acceptable. In our January survey, nearly 29% of respondents who received a product that was not what they expected said they chose to file a false item-not-received chargeback either because it wasn't clear how to return the item or that returning it was too much trouble.

The best approach to disputing chargebacks is also to be proactive. The time to start to prepare for chargebacks is now. Prepare a solid strategy with clear internal procedures and policies for managing the evidence. That means transaction data, proof of delivery, a record of customer interaction and any other evidence, such as a customer's social media declarations or photos proving they have the item they said never arrived.

Fighting a chargeback is something like going to court — complete with rules of evidence and deadlines. You need a dedicated team, either internally or externally, to be focused on monitoring, managing, and when appropriate, fighting chargebacks.

**Stefan Nandzik**
**VP of Corporate Communication, Signifyd**

Stefan Nandzik is the head of product and brand at Signifyd. His "what if" approach to business problem-solving constantly challenges conventional wisdom and means that he is never afraid to upend the status quo to lead change. Prior to joining Signifyd, Stefan ran the Global Demand Center at Citrix.

# T1 Payments

**T1 Payments is a high-risk merchant processing company that is flexible, transparent, and scalable. T1 Payments' secure gateway and integrated shopping cart solutions are compliant with all Payment Card Industry Data Security Standards (PCI DSS).**

**In addition to high-risk merchant processing services, T1 Payments stays involved in the community through its ongoing donations and sponsorships. To learn more about the nonprofits T1 Payments supports, visit T1 Payments Community Involvement page on their website.**

www.t1payments.com

## How will COVID-19 continue to influence eCommerce fraud prevention in 2021?

Fraudsters don't give up; they continually evolve. With the rise of COVID-19, we have seen a notable increase in instances of fraud. This could be a result of more time on people's hands, more resources for fraud available online, or more incentives for fraud as much of the economy moves online – or a perfect storm formed by all of these causes.

Due to the pandemic, many existing merchants have invested in moving their business online, and many new merchants have entered the eCommerce space as layoffs and social distancing have allowed more time for new ventures. However, inexperienced merchants may not be prepared for the rampant onslaught of cyberattacks.

Though many merchants do not want to believe they will be targeted by fraudsters and want to avoid upfront expenditure on fraud prevention infrastructure, many learn the hard way that protections, like biometrics and two-factor authentication (e.g. entering a PIN into your own phone to confirm a transaction) are essential for any eCommerce business.

Here are three of the most persistent methods of fraud we've seen in 2020:

- **Data breaches** – Data breaches have become unfortunately common in the last few months, most notably in the medical space but also in retail. eCommerce vendors should prepare to double-encrypt all customer data and set up powerful firewalls to protect customers' data from being stolen – and your business's reputation from being trampled.

• **Credit card testing –** Credit card testing is when a fraudster uses an eCommerce site to test stolen credit card data by making tens of thousands of tiny purchases. This allows the scammer to test which cards have been reported stolen and which are still viable to make much larger purchases. These fraudulent purchases will often take place in the middle of the night, in rapid succession, and can cripple a small eCommerce business due to enormous charge-back fees as customers have their banks request refunds. In order to foresee and prevent this form of fraud, merchants can install additional identity verification tools, such as AVS and CVV, as well as session validation. These tools should allow businesses to verify customer identity and prevent fraudsters without alienating real customers by asking them to jump through hoops.

• **Fraudulent applications and identity theft –** We have seen an unprecedented surge in fraudulent business applications, as scammers steal key identity details and then apply for a merchant account using another's credentials. To prevent this, eCommerce merchants should always give limited information upfront and get clarity on where that information will be distributed – and payments processors should carefully vet each merchant application to ensure authenticity. To ensure they are safe, merchants can contact their credit bureau to see if other inquiries were made into their credit.

## What are the trends in privacy regulation (i.e. GDPR) and payments regulation (i.e. PSD2) that will impact merchants and the eCommerce fraud prevention industry?

When it comes to fraud prevention, payments and privacy regulators don't allow the eCommerce industry to outrun the bear, but just run faster than the slowest person. These frameworks were designed with the customer in mind rather than the eCommerce vendor, which can be frustrating for merchants.

From a fraud perspective, the customer's right to delete their own data is concerning. Fraudsters could potentially delete data that can be used for fraud detection and analysis, or information that merchants could use to bolster their case in chargeback representments.

On the other hand, the General Data Protection Regulation (GDPR) has spurred improved fraud prevention and incident response strategies throughout the European eCommerce industry. In fact, some of these data regulations have opened doors for new ventures in regulatory technology (regtech), as demand for compliance services increases. Compliance regtech can help businesses automatically identify new policy requirements, embed those requirements into algorithms, and monitor for further compliance risks. Regtech helps significantly reduce manual interventions and saves merchants time to dedicate to growing their business.

Even without the threat of PSD2 enforcement, it's a good idea for merchants to implement Strong Customer Authentication (SCA), which can be done by using the widely available 3D Secure 2.0 anti-fraud protocol. This backend technology allows transaction verification between merchants and banks directly, without the customer being redirected or re-prompted. However, note that improved fraud prevention does not come without costs. Merchants who use SCA methods such as 3D Secure may find that the increased payment friction leads to a reduction in acceptance rates and may elicit some pushback from customers.

## What will be the biggest 2021 eCommerce fraud trend that is currently being overlooked?

As a result of fraud and cyberattacks, more eCommerce merchants will be designated “high-risk.”

We know that fraud will increase in 2021: more businesses are moving online, fraudsters are getting more creative, and risk and underwriting departments are being stretched thin by new demands and cost-cutting. Many merchants and fraud technologies are laser-focused on predicting fraud trends and new methods, but many are not seriously considering the domino effect of an increase in cyberattacks, aside from additional expenses. One hit targeting a business can lead to devastating chargebacks, which can lead to increased holdbacks from the payment processor, which can in turn lead to a business being declared “high-risk.”

Merchant accounts deemed “high-risk” often struggle to find a qualified payment processor willing to work with them and may also have trouble finding a banking partner to underwrite the business. Businesses designated “high-risk” will often have lower monthly processing limits, more difficulty entering certain business contracts and operating federally, and higher fees overall.

Being deemed “high risk” is certainly not the end of the world for a business, and there are many ways for businesses to handle this alternate financial designation, including by finding a processor that understands compliance and the difficulties and best practices for high-risk payment processing.

**Donald Kasdon**
**Founder, T1 Payments**

Donald Kasdon is the founder of payment processing service T1 Payments. After working at the NY Mercantile Stock Exchange, as well as in real estate and retail, he experienced first-hand the inefficiencies of the payments ecosystem. That’s why in 2012 Donald founded T1 Payments, which focuses on enabling eCommerce for all types of merchants, especially high-risk. Today, T1 Payments’ secure gateway and integrated shopping cart solutions are trusted by thousands of global organizations.

# Vesta

**Vesta is a leader in guaranteed fraud protection and e-commerce payment solutions that help online merchants, major telcos, payment processors and acquirers optimize revenue by eliminating the fear of fraud. Founded in 1995, Vesta pioneered fully guaranteed card-not-present (CNP) payment transactions for the telecommunications industry by using its cutting-edge data science and machine learning capabilities to thwart fraud and ensure that more valid transactions are approved. Today, Vesta processes and protects billions of dollars in transactions annually. The company's flexible and scalable solutions enable its customers to eliminate the fear of fraud and increase revenue by delivering secure, frictionless transactions that maximize acceptance and improve customer experience, all backed by a zero-fraud-liability guarantee.**

www.trustvesta.com

### How will COVID-19 continue to influence eCommerce fraud prevention in 2021?

The need for fraud prevention solutions today is greater than it was when the pandemic began. Many legacy merchants are still struggling to manage the shift of their business model caused by the decrease in foot traffic to physical locations and explosion of eCommerce demand. They are navigating new territory – from emerging logistics and supply chain challenges to rapidly evolving customer demands. And while the pandemic has created an eCommerce boom for many merchants, fraud has grown with it in lockstep.

With COVID-19 still keeping customers from braving potentially crowded stores for their day-to-day shopping needs, fraudsters will continue to look for new ways to exploit the increase in digital transactions. Merchants should pay close attention to any new payment methods, transaction dynamics or customer preferences that emerge during this time, as anything unusal can be a sign of fraudlent activity. It's more important than ever for merchants to deliver the best customer experience they can, and that includes ensuring fraudulent transactions are blocked while legitamte orders are approved and processed seamlessly.

### What are the trends in privacy regulation (ie. GDPR) and payments regulation (ie. PSD2) that will impact merchants and the eCommerce fraud prevention industry?

With privacy regulations like GDPR and the California Consumer Protection Act (CCPA) having placed more stringent requirements around the use and storage of consumer data, merchants have gradually moved away from the use of PII and towards more sophisticated approaches like device fingerprinting, which measures device – rather than consumer – behavior. This approach offers consumers more autonomy over their personal data and better protection in the event a merchant's network or website is breached.

However, stricter privacy regulations can also adversly affect the customer experience since they limit what kinds of consumer data merchants can access and use. This removes a layer of customization and personalization from the experience. A recent survey found 80% of U.S. consumers were in favor of federal data privacy legislation, but a different survey revealed that 80% of respondents want personalization from retailers. This clearly presents a challenge for merchants, forcing them to carefully walk the line between adhering to privacy regulation while finding new ways to make the customer experience feel bespoke.

Federal data privacy legislation has not been a priority in the U.S., but many national organizations have embraced the CCPA as a standard across all markets to make their lives easier. That said, you have to remember this is an evolving space and regulations continue to change. After the passage of Proposition 24, the California Privacy Rights Act, on election day, it appears the CPRA is poised to replace the CCPA, closing several loopholes in that legislation and making it easier for people to opt out of having their data collected or processed.

In terms of payments regulation, the pandemic has driven huge demand for contactless payments, and lawmakers are pushing to create a smarter, more flexible regulatory environment to make it easier for merchants and consumers to adopt these common sense solutions. There have also been calls to make the adoption of peer-to-peer payments easier for small business to access and use. Emerging economies around the world have been ahead of the curve there – mostly out of necessity since many of them lacked the mature banking infrastructure present across the west - and now it’s time for western econmies to catch up.

**What will be the biggest 2021 eCommerce fraud trend that is currently being overlooked?**

First, consider the explosion of account takeover attempts amid the pandemic. While the threat itself isn’t being overlooked, the processes and tooling available to merchants to detect and prevent this type of fraud do require a closer look. To effectively combat account takeovers, merchants need an orchestrated approach that combines biometric evaluations with machine learning to discover and stop account fraud in real time.

Another area that requires more attention is how the fear of fraud can be more damaging than fraud itself. Too many businesses are so hyper-focused on fraud prevention that they hurt themselves in the long run. For CNP transactions, if merchants prevent fraud by rejecting any transaction where they are not 100% certain of its legitimacy, there is a very high chance they are suppressing revenue and turning away many genuine customers. Just about every merchant out there can tell you what their fraud rate is, but relatively few know their approval rate or understand the relationship between the two. A very low fraud rate is not necessarily a good thing, as it could indicate the merchant is rejecting an outsized number of transactions. Most merchants don’t know how much revenue they turn away through their fear of fraud, but some analysts estimate lost revenue through false declines is more than 10x the amount of actual fraud losses. This is a lot more damaging than many merchants recognize; in a recent survey of U.S. consumers, 33% said they would never again shop with a merchant if it had falsely declined their payment. Merchants need to realize the impact this has on their business and shift their perspective to avoid letting the fear of fraud thwart long-term growth.

Fraudsters will always innovate and find new services or channels to exploit, but we will eventually shift from prioritizing effective fraud detection to more of a fraud recognition mindset. Until we get there with AI, merchants should stop holding themselves to the unrealistic goal of achieving zero fraud. Rather, they should start thinking about fraud in a more balanced way and keep an eye on the relationship between fraud rates and approval rates.

**Ron Hynes,**
**Vesta CEO**

Ron Hynes, CEO at Vesta, has a 20-year track record of leading and scaling high-growth payment businesses. His background spans a variety of established and startup fintech companies, including four years at the helm of Mastercard's global prepaid business, where he led remarkable global revenue and market share growth. Most recently, as CEO of UniRush, he led the turnaround and eventual sale of the company and its RushCard business to GreenDot. At Vesta, Hynes is charged with leading the company as it pursues an aggressive expansion agenda on both product and geographic fronts.

# Summary Conclusion: Our E-commerce Fraud Prevention Predictions for 2021

2020 has been a year unlike any other. Lives, industries, and businesses have been forever changed. However, it's also brought a chilling truth to light: There are still people out there ready and willing to take advantage of the situation. Fraudsters have no shame.

Merchants must be prepared for this on several fronts in 2021.

First, the motivation and preparation factor. While businesses have spent most of the year adapting on the fly to ever-changing circumstances, fraudsters have been seeing opportunities to attack. Vulnerabilities exist in backend systems set up quickly to handle surplus orders; managers incentivized to hit revenue targets that don't take fraud into account; employees overworked, overstressed, and exhausted from handling one crisis after another since March.

Second, the regulatory environment remains fluid. Lawmakers in the United States and Europe have awoken to big tech's hold on big data. Directives like GDPR and PSD2 will increase in scope, placing an additional regulatory burden on merchants. Additional legislation is not unthinkable. Merchants will most likely need to navigate an increasingly strict set of privacy and security rules.

Third, the pandemic has accelerated the transition to ecommerce. Change anticipated to occur over the course of 5 years has happened in as many months. Merchants will face continuing pressure to prevent fraud as order volumes increase. Onboarding new technology, re-thinking how to organize fraud departments, and reviewing policies will be more important than ever.

In our 2020 guide, we wrote: "2020 is probably the year they begin to wax nostalgic about the days when all they needed to worry about was CNP fraud."

We were right in more ways than one. Now, as the change set in motion by the pandemic continues, we expect the combination of more sophisticated attacks, additional regulation, and increased order volumes to be the defining characteristics of 2021.

**~ The Editorial Board**

*“If everyone is moving forward together, success takes care of itself”*

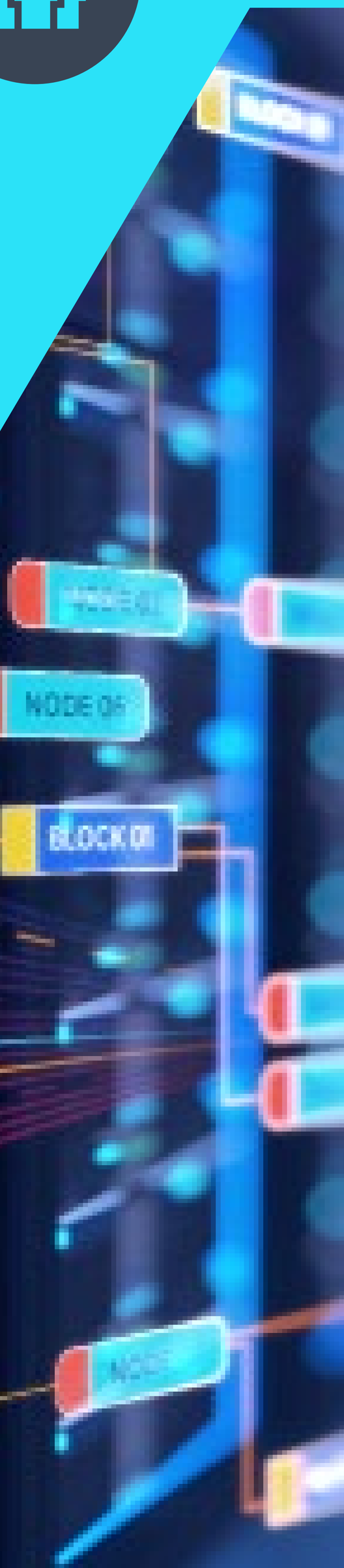
**Henry Ford**

# About MFJ

Merchant Fraud Journal is an independent and unbiased publication dedicated to empowering online sellers to greatly reduce the impact of eCommerce fraud on their businesses. Its core mission is to break the silos surrounding merchants' internal fraud prevention processes by bringing together industry professionals to share their knowledge with one another.

Unfortunately, the business process knowledge needed for online sellers to greatly reduce the impact of eCommerce fraud is scarcely available right now. There is no single forum and resource where merchants, payment professionals, and other industry professionals could go to get educated on the myriad of challenges they face.

We seek to fill that gap by being a resource that collects insight from industry thought leaders and fraud prevention tool experts on topics such as chargebacks, false positive declines, account takeover fraud, friendly fraud, data breaches and more. Our goal is to help honest businesses quickly understand their security options and take action, so they can get back to focusing on their core business activities.



## LIKE OUR REPORT?
## CONTACT US

Looking to create custom content, research, and reports that influence eCommerce and retail industry decision makers?

---

Connect with us for more details:
Dan Moshkovich,
Founder & CEO
Dan@merchantfraudjournal.com

## WANT TO CONTRIBUTE?
## CONTACT US

Want to share editorial content and contribute to Merchant Fraud Journal?

---

Connect with us for more details:
Bradley Chalupski,
Founder & Editor-in-chief
Bradley@merchantfraudjournal.com


Merchant Fraud Journal

290 Caldari Road,
Concord, Ontario L4K 4J4
Canada
--

hello@merchantfraudjournal.com

www.merchantfraudjournal.com

1-(888) 225-2909