



PayPal Certified Developer Program Study Guide

For Professional Use Only
Currently only available in English.

A usage Professional Uniquement
Disponible en Anglais uniquement pour l'instant.

PayPal Certified Developer Program Study Guide

Document Number: 100018.en_US-200803

© 2008 PayPal, Inc. All rights reserved. PayPal is a registered trademark of PayPal, Inc. The PayPal logo is a trademark of PayPal, Inc. Other trademarks and brands are the property of their respective owners.
The information in this document belongs to PayPal, Inc. It may not be used, reproduced or disclosed without the written approval of PayPal, Inc. PayPal (Europe) Ltd. is authorised and regulated by the Financial Services Authority in the United Kingdom as an electronic money institution. PayPal FSA Register Number: 226056.

Notice of non-liability:

PayPal, Inc. is providing the information in this document to you "AS-IS" with all faults. PayPal, Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. PayPal, Inc. assumes no liability for damages (whether direct or indirect), caused by errors or omissions, or resulting from the use of this document or the information contained in this document or resulting from the application or use of the product or service described herein. PayPal, Inc. reserves the right to make changes to any information herein without further notice.



Contents

Chapter 1 Online Payment Processing 11

Online Selling Basics.	11
The Payment Processing Network.	11
Individuals	12
Institutions	12
Processes and Services	12
How Online Payment Processing Works.	12
Payment Processing Authorization	12
Payment Processing Settlement.	13
What to Look for in an Online Payment Processing Solution	13
PayPal's Payment Processing Solutions.	14
Review Questions	18

Chapter 2 Internet Security and Fraud Prevention 23

Why Every Business Should Be Concerned About Internet Fraud	23
Liability for Internet Fraud	24
Internet Fraud: What It Is and How It Happens	25
Who Is at Risk for Online Fraud	26
Reducing Exposure to Fraud.	27
What Banks and Card Associations Are Doing to Prevent Online Credit Card Fraud	28
What PayPal Is Doing to Protect Your Business Against Fraud	29
How to Reduce Chargebacks	29
Disclosure and Compliance	30
Disclosure Policy.	30
PCI Data Security Standard Compliance	31
Additional Resources About Disclosure and Compliance	33
PayPal Fraud Protection Services	34
Detailed Service Descriptions	34
PayPal Fraud Protection Services Upgrade Options	36
Review Questions	37

Chapter 3	Getting Started With Account Setup	. 43
	Basic Steps for Getting Started	43
	PayPal Sandbox	44
	Review Question	45
Chapter 4	API Credentials	. 47
	What API Credentials Are	47
	Choosing an Authentication Method	47
	Establishing API Credentials	48
	API Signature	48
	API Certificate	48
	Using API Credentials	50
	Review Questions	51
Chapter 5	Name-Value Pair (NVP) API	. 53
	Integrating with the PayPal API	53
	Basic Steps	53
	Create a Web Application	53
	Get API Credentials	53
	Create and Post the Request	54
	Interpret the Response	54
	Technical Details	54
	Request-Response Model	54
	Request Format	56
	Response Format	57
	Posting Using HTTPS	58
	Review Questions	58
Chapter 6	Express Checkout	. 59
	How Express Checkout Works	59
	Express Checkout API Reference Information	61
	SetExpressCheckout Request	62
	SetExpressCheckout Response	65
	GetExpressCheckoutDetails Request	66
	GetExpressCheckoutDetails Response	66
	DoExpressCheckoutPayment Request	68
	DoExpressCheckoutPayment Response	71

Button and Logo Placement and Use	73
PayPal Button as a Checkout Choice	74
PayPal Button as a Payment Method	74
Using PayPal-Hosted Images	75
Tips	75
Redirecting to PayPal	75
Recommendation for Browser Redirection	75
Order Review Page Setup	76
Authorization & Capture	76
Review Questions	77
Chapter 7 Direct Payment API	79
How Direct Payment Works	79
Direct Payment API Reference Information	80
DoDirectPayment Request	80
DoDirectPayment Response.	84
Authorization & Capture	85
Review Questions	85
Chapter 8 Transactions	87
Authorization & Capture APIs	87
Authorization Process	87
Honor Period and Authorization Period	88
Authorization & Capture API Reference Information	88
Authorization & Capture Best Practices	93
For More Information	93
Refunds	93
RefundTransaction Request	94
RefundTransaction Response	94
Transaction Searches	95
TransactionSearch Request	95
TransactionSearch Response	98
Retrieving Transaction Details	98
GetTransactionDetails Request	99
GetTransactionDetails Response	99
Payment Notification Integration	99
Email	99
Reporting	100

Instant Payment Notification (IPN)	.100
Dispute Notification	.103
Review Questions	.103
Chapter 9 Sandbox Testing	.105
Overview	.105
At a Glance: Differences between the Sandbox and Live PayPal	.105
Accessing the PayPal Sandbox	.107
Signing Up for Sandbox Access	.108
Welcome to the PayPal Sandbox	.110
Test Email	.110
Setting Up Test Accounts	.111
Planning the Types of Test Accounts You Need	.111
Managing Test Accounts	.112
Adding a Funding Source	.115
Signing Up for Website Payments Pro	.117
Testing PayPal Website Features	.118
Website Payments with the “Buy Now” Button	.118
Handling Pending Transactions	.120
Instant Payment Notification (IPN)	.121
Verifying a Test Refund	.122
Transferring Funds to a Test Account	.122
Clearing or Failing Test eCheck Transactions	.123
Sending Funds to a Seller	.123
Billing A Customer	.124
Testing PayPal NVP APIs	.125
Testing Express Checkout	.126
Testing Error Conditions	.129
API Testing	.130
Testing Using AVS Codes	.134
Testing Using CVV Codes	.138
Testing Recurring Payments	.140
Review Questions	.141
Appendix A Answers to Review Questions	.143
Chapter 1	.143
Chapter 2	.146
Chapter 3	.150



- Chapter 4.151
- Chapter 5.151
- Chapter 6.151
- Chapter 7.151
- Chapter 9.152

- Appendix B General Reference Information 153**
 - ShippingAddress Parameter153
 - PayPal-Supported Transactional Currencies154
 - AVS Response Codes155
 - CVV2 Response Codes156

- Glossary 157**

- Index. 159**



List of Tables

Table 1.1	PayPal Payment Processing Solutions	17
Table 2.1	High Fraud Risk Quick Reference	26
Table 2.2	PCI Data Security Standard	32
Table 2.3	Merchant Levels for PCI Compliance	32
Table 2.4	PCI Compliance Validation Requirements	33
Table 2.5	Fraud Protection Services Purchase Options	34
Table 2.6	Comparison of Fraud Protection Services	35
Table 4.1	Required Security Parameters	50
Table 5.1	URL-Encoding Methods	55
Table 5.2	General Format of a Request	56
Table 5.3	General Format of a Successful Response	57
Table 5.4	ACK Parameter Values	57
Table 5.5	Format of an Error Response	57
Table 6.1	Express Checkout Flow-of-Control and Integration Points	60
Table 6.2	SetExpressCheckout Request Parameters	62
Table 6.3	SetExpressCheckout Response Fields	65
Table 6.4	GetExpressCheckoutDetails Request Parameters	66
Table 6.5	GetExpressCheckoutDetails Response Fields	66
Table 6.6	DoExpressCheckoutPayment Request Parameters	68
Table 6.7	DoExpressCheckoutPayment Response Fields	71
Table 7.1	DoDirectPayment Request Parameters	80
Table 7.2	DoDirectPayment Response Fields	84
Table 8.1	DoCapture Request Parameters	88
Table 8.2	DoCapture Response Fields	89
Table 8.3	DoVoid Request Parameters	91
Table 8.4	DoVoid Response Fields	92
Table 8.5	DoReauthorization Request Parameters	92
Table 8.6	DoReauthorization Response Fields	92
Table 8.7	RefundTransaction Request Parameters	94
Table 8.8	RefundTransaction Response Fields	94
Table 8.9	TransactionSearch Request Parameters	95

Table 8.10	TransactionSearch Response Fields	98
Table 8.11	GetTransactionDetails Request Parameters	99
Table 9.1	Differences between PayPal Sandbox, and Live PayPal	105
Table 9.2	API Fields That Trigger Error Conditions	130
Table 9.3	AVS Error Conditions and Triggers	134
Table 9.4	CVV Error Conditions and Triggers	138
Table B.1	ShippingAddress	153
Table B.2	PayPal-Supported Currencies and Currency Codes for Transactions	154
Table B.3	AVS Response Codes	155
Table B.4	CVV2 Response Codes	156

1

Online Payment Processing

Online payment processing simplifies the operation of an online store by providing a reliable, easy, secure, and seamless experience for merchants and customers.

In this chapter, you will learn:

- Online payment processing basics
- How the payment processing network operates
- How payment processing works
- What to look for in an online payment processing solution
- PayPal's payment processing solutions

Online Selling Basics

With the right payment processing services, online merchants can get paid quickly and easily while protecting themselves against fraud. The most critical step in establishing an online store is ensuring that you can accept customer payments for single or repeated transactions. Online payment processing tools offer customers the convenience of paying by credit card, PayPal®, or other electronic payment sources like debit cards, purchase cards, and eChecks.

Additionally, successful online merchants must make sure their stores are secure. Online fraud rates are climbing, but smart merchants can protect themselves with security and fraud prevention systems from a company they trust. According to CyberSource Corp., businesses lost nearly \$2.8 billion USD to online fraud in 2005, up from \$2.6 billion USD in 2004. PayPal's Fraud Protection Services provide secure and reliable tools that offer peace of mind.

The Payment Processing Network

The payment processing network connects sellers, buyers, and banks to enable the secure and reliable execution of online transactions. Sellers need an internet merchant account with an acquiring bank that allows them to accept customer credit cards electronically. Customers need a bank that issues credit cards and verifies the customer's credit limit and available cash balance for proposed purchases. The elements and participants include individuals, institutions, and processes and services.

Individuals

- **Merchant:** Someone who sells goods or services.
- **Customer:** The holder of the payment instrument.

Institutions

- **Customer issuing bank:** The institution providing the customer's credit card.
- **Acquiring bank:** Provides internet merchant accounts required to enable online card authorization and payment processing.
- **Credit card associations:** Financial institutions that provide credit card services in concert with credit card associations such as Visa and MasterCard.
- **Processor:** A large data center that processes credit card transactions and settles funds for merchants. A processor can be either a bank or a company dedicated to providing these services. Ceridian is an example of a payment processor.

Processes and Services

- **Authorizations:** The process of verifying that customer credit cards are active and have sufficient available credit limits.
- **Settlements:** Processing authorized transactions to settle funds into a merchant's account.
- **Payment processing service:** A service that connects merchants, customers, and banks involved in online transactions. A third party, such as PayPal with its secure payment gateway, usually offers this service.

How Online Payment Processing Works

Online payment processing consists of two principal steps: authorization and settlement. Authorization verifies that the card is active and the customer has sufficient credit to make the transaction. Settlement is the process of charging the customer's card account and transferring money from the customer's account to the merchant's account.

Payment Processing Authorization

During authorization, a bank verifies that holders of a payment instrument, like a credit card, have sufficient credit or funds to make a purchase. The payment authorization process engages multiple institutions and services to verify that sufficient credit is available to complete the transaction as follows:

1. Customer decides to purchase online and inputs credit card information.

2. Merchant's website receives customer information and sends it to payment processing service.
3. Processing service routes information to processor.
4. Processor routes information to bank that issued customer's credit card.
5. Issuing bank sends authorization (or declination) to processor.
6. Processor routes transaction results to payment processing service.
7. Processing service sends results to merchant.
8. Merchant decides to accept or reject purchase. (Here, the merchant should take additional precautions to ensure the credit card is not stolen and that the customer actually owns this card.)

Payment Processing Settlement

Once the merchant has shipped the product or authorized the download of merchandise, the merchant may request that the payment processing service settle the transaction. During settlement, funds are transferred from the customer's account to the merchant's bank account.

1. Merchant informs the payment processing service to settle transactions.
2. Payment processing service sends transactions to processor.
3. Processor checks the information, and forwards settled transaction information to the card association and card-issuing bank.
4. Transactions are settled to the card issuers and funds move between the acquiring bank and issuing bank. Funds received for these transactions are sent to the merchant's bank account.
5. Acquiring bank credits merchant's bank account.
6. Issuing bank includes merchant's charge on customer's credit card account.

What to Look for in an Online Payment Processing Solution

Finding a reliable, secure, and flexible payment processing solution is critical. A payment processing solution should be:

Secure

- Backed by an established, trustworthy company
- Comply with the Payment Card Industry (PCI) Data Security Standard
- Provide comprehensive and standard antifraud features
- Store customer financial information with state-of-the-art encryption
- Supply password-protected account management

Reliable

- Provide reliable and cost-effective acceptance and processing of a variety of payment types
- Authorize credit cards in real time
- Scale to thousands of transactions to meet peak demand
- Based on a fault-tolerant network of redundant servers to ensure uninterrupted operations

Easy to Use

- Provide easy, flexible integration with merchant's website
- Scale rapidly and seamlessly as transaction volume increases
- Work with leading internet merchant account providers
- Provide easy-to-use tracking and reporting system
- Store transaction records securely
- Process offline transactions through a virtual terminal
- Provide recurring billing payment for services
- Offer upgrade options to accommodate future growth

PayPal's Payment Processing Solutions

PayPal's payment processing solutions are designed to meet the demanding and diverse needs of a variety of online merchants. By providing affordable payment connections among merchants, customers, and financial networks, PayPal's solutions take advantage of the latest technical resources to streamline transactions, while helping to prevent fraud. Products including Payflow Link, Payflow Pro, Website Payments Standard, and Website Payments Pro allow everyone from mom-and-pop online retail stores to enterprise-level businesses to process transactions easily, reliably, and securely.

PayPal's Fraud Protection Services and Recurring Billing Service for Payflow, along with other customer service packages, include professional integration support. Most importantly, Payflow offers one of the industry's few payment processing services with immediate connectivity to all major processors and most shopping carts. Note, however, that you do not need a PayPal account to process credit cards on your website.

Once you have your own website, ask a few simple questions to determine which product is right for you:

1. Do you need an all-in-one solution that includes an internet merchant account and allows you to process credit cards online?

If you don't have your own internet merchant or business bank account, PayPal can provide a total solution with its Website Payments Standard and Website Payments Pro solutions:

- **Website Payments Pro:** Website Payments Pro is an all-in-one payment solution that allows customers to shop and pay on your site. You can accept credit cards directly on

your site and get the features of a merchant account and gateway through a single provider at a lower cost. Website Payments Pro allows you to control your checkout from start to finish.

For more information on Website Payments Pro, go to: https://www.paypal.com/cgi-bin/webscr?cmd=_wp-pro-overview-outside.

- **Website Payments Standard:** Website Payments Standard lets customers shop on your website and pay on PayPal. It offers a pay-per-use model with no set-up or monthly fees. Like Website Payments Pro, it includes shipping and tax calculators, reporting tools to measure your business, and support for international currencies.

For more information on Website Payments Standard, go to:

https://www.paypal.com/cgi-bin/webscr?cmd=_wp-standard-overview-outside.

2. Do you have your own internet merchant account or business bank account that allows you to process credit cards online?

If you do, consider PayPal Payflow Gateway products. A gateway provides a secure connection between your online store and your internet merchant account.

- **Payflow Pro:** Scalable and fully customizable, the Payflow Pro solution is recommended for merchants who require peak site performance and direct control over payment functionality on their site. Merchants using this service can enhance the customer experience by allowing shoppers to complete the checkout process without ever leaving your site.

For more information on Payflow Pro, go to: https://www.paypal.com/cgi-bin/webscr?cmd=_payflow-pro-overview-outside.

- **Payflow Link:** This service is designed for merchants who require a simple solution to selling on the web. In order to use this service, you need to add only a small piece of HTML code that will link your customers to order forms hosted by PayPal. This simple package allows you to process payments by credit cards, debit cards, and checks, online and offline. It also works with most major shopping carts.

For more information on Payflow Link, go to: https://www.paypal.com/cgi-bin/webscr?cmd=_payflow-link-overview-outside.

3. Do you need a basic payment processing service?

Look first to a basic PayPal service for processing credit cards payments. These include:

- **PayPal Email Payments:** Email Payments lets you send customers email invoices that they can pay on PayPal. This simple solution does not require you to have a shopping cart or an internet merchant account.

For more information on PayPal Email Payments, go to: https://www.paypal.com/cgi-bin/webscr?cmd=_email-payments-overview-outside.

- **PayPal Virtual Terminal:** Virtual Terminal provides your business with the same functionality as a stand-alone credit card-processing terminal, but allows you to accept credit card payments by phone, fax, and email. You can use Virtual Terminal on any computer with an internet connection.

For more information on PayPal Virtual Terminal, go to: https://www.paypal.com/cgi-bin/webscr?cmd=_vt_hub-outside.

- **PayPal as an Additional Payment Option:** This option allows merchants to put the PayPal logo on their own website to accept PayPal as an alternative payment source, in addition to credit cards such as MasterCard® or Visa®.

For more information on PayPal as an Additional Payment Option, go to:

https://www.paypal.com/cgi-bin/webscr?cmd=_additional-payment-overview-outside.

TABLE 1.1 PayPal Payment Processing Solutions

I need an all-in-one solution		I have an internet merchant account		I need basic payment processing		Additional payment option	
Website Payments Pro	Website Payments Standard	Payflow Pro	Payflow Link	Email Payments	Virtual Terminal	PayPal	
Customer Experience							
Where customers shop:	Shop on merchant website	Shop on merchant website	Shop on merchant website	Shop on merchant website	Varies with merchant business	Varies with merchant business	Shop on merchant website
Where customers check out:	Merchant website or on PayPal	PayPal	Merchant website or on PayPal	PayPal	PayPal	Phone, fax, or mail	PayPal
Customers need a PayPal account:	No	No	No	No	No	No	No
Integration							
Internet merchant account:	Included	Not needed	Required	Required	Not needed	Included	Required
Shopping cart support:	Yes	Yes	Yes	Yes	Not required	Not required	Yes
Technical skills:	APIs	HTML	APIs or HTML	APIs or HTML	Not required	Not required	APIs or HTML
Ability to accept phone, fax, or mail orders	Included	Upgrade	Included	Included	Upgrade	Included	Upgrade

NOTE: This Study Guide and the PayPal Developer Certification cover the Website Payments Pro solution with Express Checkout.

Review Questions

Answers to review questions are in [Appendix A, “Answers to Review Questions.”](#)

1. Indicate if each statement is True (T) or False (F).

- The most critical step in establishing an online store is ensuring that you can accept customer payments for single or repeated transactions.
- According to Cybersource Corp., businesses lost nearly \$2.8 billion USD to online fraud in 2005, down from \$3.0 billion USD in 2004.
- The payment processing network connects buyers, sellers, and banks to enable the secure and reliable execution of online transactions.
- By providing affordable payment connections among merchants, customers, and financial networks, PayPal’s solutions take advantage of the latest technical resources to streamline transactions, while helping to prevent fraud.

2. Match each participant in the payment processing network to the role they perform.

Response	Participant	Role Performed
	Merchant	1. The holder of the payment instrument.
	Customer	2. A financial institution that provides credit card services in concert with credit card associations such as Visa and MasterCard.
	Customer Issuing Bank	3. Someone who sells goods or services.
	Acquiring Bank	4. A large data center that processes credit card transactions and settles funds for merchants.
	Credit Card Association	5. An institution that provides merchant accounts required to enable online card authorization and payment processing.
	Processor	6. The institution providing the customer’s credit card.

3. The following steps describe the payment authorization process. Indicate the correct order of the steps by placing the step number to the left of each description.

Processor routes information to bank that issued customer's credit card.
 Merchant's website receives customer information and sends it to payment processing service.
 Processing service sends results to merchant.
 Merchant decides to accept or reject purchase.
 Customer decides to purchase online and inputs credit card information.
 Processor routes transaction results to payment processing service.
 Processing service routes information to processor.
 Issuing bank sends authorization (or declination) to processor.

4. The following steps describe the payment processing settlement process. Indicate the correct order of the steps by placing the step number to the left of each description.

Acquiring bank credits merchant's bank account.
 Merchant informs the payment processing service to settle transactions.
 Processor checks the information, and forwards settled transaction information to the card association and card-issuing bank.
 Issuing bank includes merchant's charge on customer's credit card account.
 Transactions are settled to the card issuers and funds move between the acquiring bank and issuing bank. Funds received for these transactions are sent to the merchant's bank account.
 Payment processing service sends transactions to processor.

5. Finding a reliable, secure, and flexible payment processing solution is critical. What features should a payment processing solution offer? (Select all that apply.)

Backed by an established, trustworthy company
 Comply with Payment Card Industry (PCI) Data Security Standard
 Store customer financial information in plain sight
 Authorize credit cards in real time
 Based on a network that provides near real-time credit card transactions
 Scale rapidly and seamlessly as transaction volume increases
 Offer upgrade options to accommodate future growth
 Provide recurrent billing payment for service

6. Match each PayPal solution to the service it offers.

Response	PayPal Product	Service Description
	Website Payments Pro	1. Lets you send customers email invoices that they can pay on PayPal. This simple solution does not require you to have a shopping cart or an internet merchant account.
	Website Payments Standard	2. A gateway that provides a secure connection between your online store and your internet merchant account. Scalable and fully customizable, this solution is recommended for merchants who require peak site performance and direct control over payment functionality on their site. Merchants using this service can enhance the customer experience by allowing shoppers to complete the checkout process without ever leaving your site.
	Payflow Pro	3. Allows merchants to put the PayPal logo on their own website to accept PayPal as an alternative payment source, in addition to credit cards such as MasterCard® or Visa®.
	Payflow Link	4. An all-in-one payment solution that allows customers to shop and pay on your site. You can accept credit cards directly on your site and get the features of a merchant account and gateway through a single provider at a lower cost.
	PayPal Email Payments	5. A gateway that provides a secure connection between your online store and your internet merchant account. This service is designed for merchants who require a simple solution to selling on the web. In order to use this service, you need to add only a small piece of HTML code that will link your customers to order forms hosted by PayPal.
	PayPal Virtual Terminal	6. Provides your business with the same functionality as a stand-alone credit card-processing terminal, but allows you to accept credit card payments by phone, fax, and email.
	PayPal as an Additional Payment Option	7. Lets customers shop on your website and pay on PayPal. It offers a pay-per-use model with no set-up or monthly fees. It includes shipping and tax calculators, reporting tools to measure your business, and support for international currencies.

7. Select the PayPal payment processing solutions that enable a customer to checkout on the merchant's website.

Website Payments Pro
 Website Payments Standard
 Payflo Pro
 Payflow Link
 Email Payments
 Virtual Terminal
 PayPal as an Additional Payment Option

8. Select the PayPal payment processing solutions that require API or HTML technical skills to develop payment processing applications.

Website Payments Pro
 Website Payments Standard
 Payflo Pro
 Payflow Link
 Email Payments
 Virtual Terminal
 PayPal as an Additional Payment Option

2

Internet Security and Fraud Prevention

E-commerce has become an essential sales channel for businesses both domestically and internationally. Unfortunately, e-commerce has also become an attractive revenue source for criminals who perpetrate internet fraud. You need to be aware and informed so that you can take steps to protect your business. Security for online payments is everyone's responsibility.

In this chapter, you will learn about:

- Why every merchant should be concerned about internet fraud
- Liability for internet fraud
- Internet fraud: What it is and how it happens
- Who is at risk for online fraud
- How to reduce your exposure to fraud
- What banks and credit card associations are doing to prevent online credit card fraud
- What PayPal is doing to protect your business against fraud
- Providing disclosure to your customers and compliance with the Payment Card Industry (PCI) standard
- PayPal® Fraud Protection Services

Why Every Business Should Be Concerned About Internet Fraud

Every merchant is at risk for fraud. When doing business online, you should be particularly aware of fraud.

Offline merchants can see who they are doing business with, look at their customers' credit cards, and watch them sign the receipt. In the online world, however, customers never sign a paper receipt, so authentication becomes a challenge. Moreover, in the online world, hackers can break into your network without your knowledge and steal money, products, and sensitive information. They can also steal customer identities and commit crimes against other merchants, using your business as a launch pad for further crimes.

Internet fraud is also more difficult to detect than in the brick-and-mortar world. Criminals who break into a physical store are much more visible than criminals who break in through the web and erase their footprints. Additionally, in the online world, criminals have multiple access points for break-ins, because the merchant store is networked internally and to other businesses.

Because of these vulnerabilities, total losses from online payment fraud have steadily increased. According to CyberSource's 2006 Online Fraud Report, an estimated \$2.8 billion USD was lost to online fraud in the U.S. and Canada in 2005. The Nilson Report, a payment

trade publication, estimates the rate of credit card fraud to be 18 cents to 24 cents per \$100 USD of online sales – three to four times higher than the overall fraud rate.

The threat of online fraud is so pervasive that the U.S. government now mandates security requirements for businesses that handle financial information online. Today these regulations apply mainly to the banking community, but as an internet merchant you access the financial networks for each transaction made on your site. As a result, security at the point of sale is becoming an increasing concern for both credit card associations and the government.

Credit card associations, for their part, hold merchants liable for fraudulent transactions because the credit card isn't physically present during online purchases. So merchants must take additional steps against online fraud. Credit card associations can impose stiff penalties for fraud – expenses on top of stolen goods and related shipping costs.

Moreover, American Express, Diners Club, Discover Card, JCB, MasterCard International and Visa U.S.A. have adopted the Payment Card Industry (PCI) Data Security Standard developed to protect account and transaction information of cardholders. The PCI standard requires merchants to adhere to a set of information security requirements or risk substantial fines. Security must therefore be a key concern.

Liability for Internet Fraud

In the offline world, you can take steps to safeguard your transactions by getting a signature and authorization, thereby shifting the liability of the transaction to the card issuer. In the online world, the liability for a fraudulent transaction always rests squarely with the merchant. Online transactions are considered card-not-present transactions and are inherently riskier. The financial consequences for a merchant who processes a fraudulent online transaction can be significant:

- Inventory loss and shipping costs for physical goods that are fraudulently purchased and then delivered
- Chargeback penalties assessed by the acquiring bank of \$15-\$30 USD per fraudulent transaction

According to Gartner Group estimates, merchants reject an estimated 5% of all transactions out of suspicion of fraud, while only 2% of transactions are actually fraudulent. The result is a significant amount of lost sales (up to 3% of sales volume) in an attempt to reduce fraud risk.

In addition to losing product and paying chargeback penalties, your business also faces costs due to fraud:

- Higher discount rates assessed as a result of processing fraudulent payments
- Labor cost for the merchant to investigate and resolve the chargeback
- Five- to six-figure card association fines or cancellation of a merchant's account when card fraud rates are consistently high

Implementing better tools and raising awareness can help you reduce lost revenue by turning away fewer legitimate customers who seem suspicious. You can also resolve chargebacks

more quickly, thus saving time and money. In some cases, online merchants have reduced their chargeback rate from 7% to 2%.

Internet Fraud: What It Is and How It Happens

All internet payment fraud is based on stolen consumer or merchant identities. It also requires access to payment networks to complete the fraud. The result is product theft, identity theft, and cash theft.

- **Product Theft:** Occurs when a criminal uses stolen credit card information to purchase goods and services.
- **Identity Theft:** Occurs when stolen credit card information is combined with readily available social security numbers and address information to open new credit cards under the victim's name and address.
- **Cash Theft:** Occurs when criminals break into a virtual cash register by stealing merchant account access information and impersonating you in order to issue credits or payments to themselves.

Fortunately, there are ways to protect against fraud. The most important thing you can do is choose a reliable and secure payment solution that includes basic and advanced antifraud features. Here are some of the most common fraud-related risks facing online merchants:

Consumer Identity Theft

Criminals steal consumer credit card information through a variety of methods, including dumpster diving for paper receipts, hacking into e-commerce networks, or using handheld "skimmers" to digitally scan numbers from credit cards of unsuspecting people at restaurants or cash registers. Phishers, meanwhile, will send fraudulent emails to consumers warning, for instance, of a problem with a credit card account in an attempt to trick the person to provide personal information. Once they've obtained the credit card information, these criminals can use it to steal products outright or open other accounts by impersonating the victim.

Merchant Identity Theft

Just as offline criminals can break into a cash register, online criminals can hack into the accounts of web merchants and funnel money to themselves. These criminals might be employees or visitors to a building who copy unprotected login information. They then can use the information to hack into a back-end system to hijack a merchant's payment gateway account, which provides the secure connection between your online store and your internet merchant account. Through this move, they can steal cash directly from the business by issuing themselves credit cards and payments.

Accessing Payment Networks

Once criminals have stolen an identity, they may access a payment network to complete the fraud. Most do this through two primary channels: a web merchant's checkout page or a payment gateway account. Although a checkout page provides convenience for both buyer and seller, it can raise some security concerns. For example, some criminals use the page to test

stolen credit cards. For the merchant, it is crucial to use products with built-in fraud protection to prevent this sort of digital theft.

Chargebacks

Chargebacks occur when a cardholder disputes a credit card purchase. During such disputes, the card-issuing bank initiates a chargeback against the merchant, retrieving the funds for the sale from the merchant's bank account. The bank initiating the chargeback is not required to notify the merchant or the merchant bank. Proving that the disputed transaction was legitimate can cost merchants significant time and resources, so keeping chargebacks to a minimum is essential. Chargebacks can hurt a merchant's bottom line by lowering its credit rating, diverting resources to resolve the dispute, and siphoning revenue from lost goods and shipping costs. The most common type of chargeback occurs when the customer:

- Did not receive the item ordered
- Did not receive the item believed to be ordered
- Had his or her credit card stolen and used by the thief
- Stole merchandise or services through the fraudulent use of a chargeback

Who Is at Risk for Online Fraud

Fraud can happen to any merchant at any time, and a single fraud incident can be enough to put a merchant out of business. That said, some merchants are at greater risk for certain types of fraud than others. PayPal has put together the following quick reference to identify some of the higher-than-average risk categories.

TABLE 2.1 High Fraud Risk Quick Reference

Merchant Type	Potential Risk
Merchants with vulnerable security defenses	Criminals take advantage of sophisticated spidering techniques to identify merchants with network vulnerabilities, and can then break into your network to steal account access information for hijacking or merchant takeovers.
High-visibility merchants	Fraud attempts are higher for merchants who advertise heavily or are in the news because criminals know that merchants who experience high transaction volumes have less time to defend against fraud.
Products/Services Sold	Potential Risk
High-ticket physical goods that are easily resold	These items, including luxury goods, computers, and other electronic equipment, are most attractive to criminals.
Goods that can be downloaded from the internet	The purchase of these goods doesn't require physical address information, making it easier for criminals to disguise a fraudulent transaction.

TABLE 2.1 High Fraud Risk Quick Reference

Customer Base	Potential Risk
International	It is difficult to validate the address or identity of foreign buyers, and it is more difficult to investigate and prosecute fraudulent activity from an overseas source.
Sales Season	Potential Risk
Heavy proportion of fourth quarter sales	Criminals know that you have limited time for fraud protection when sales volumes are high. That's why internet fraud triples in the fourth quarter.
Special promotions	Criminals watch for special offers. They know that you have limited time for fraud protection measures when sales volumes are high.

Reducing Exposure to Fraud

It is possible to significantly reduce your exposure to fraud. There are essentially three levels of exposure to fraud on the internet: the individual transactions, the payment gateway account, and the merchant network. Protecting your business from fraud requires that you address each of these levels in an integrated manner.

Transaction Level

Ensure that each transaction you accept and process is valid. You should also be careful not to deny suspicious transactions that are actually valid.

Authenticate buyers when possible. This includes understanding who your repeat customers are and keeping lists of repeat customers who have legitimately transacted on your site. Make sure all customer information is encrypted and stored safely. Also, take advantage of MasterCard® and Visa® buyer authentication programs to authenticate customers and reduce your liability.

Screen orders for fraud patterns. There is a wealth of information associated with each transaction that can help you understand the risk level. To effectively manage all the risk information associated with a transaction, it is important to use a rules engine. A rules engine automates the process of transaction screening so that you quickly fulfill orders for good customers and proactively block risky orders. PayPal Fraud Protection Services allows you to cost-effectively deploy a rules engine as well as benefit from PayPal's continuously updated lists of high-risk indicators.

Review suspicious transactions. Finally, review each transaction that is suspicious to make sure you are doing business with a legitimate customer. Online merchants today reject 5% of all transactions because they do not have the time or information to determine whether a suspicious transaction is actually a good one. PayPal Fraud Protection Services allows you to

automatically and continuously review only the suspicious orders, before you process them, allowing time to make an informed decision.

Account Level

Make sure that only authorized users have access to your payment gateway account, and be alert for suspicious account access patterns.

Lock down administrative access. With PayPal Fraud Protection Services, you can limit access to high-risk administrative transactions, such as issuing credits. You should also change your account password on a regular basis.

Monitor account level activity for suspicious patterns. Watch your account for signs of unauthorized access, which could indicate merchant account takeover. Account Monitoring from PayPal offers affordable, customized, live account monitoring staffed by experienced fraud professionals. The service can help you catch account takeover before it does any damage, whether the takeover is due to a hacker or fraudulent employee usage of your service.

Network Level

Ensure your network or “perimeter” is defended against unauthorized access.

Lock down network access. With PayPal Manager, you can ensure that only IP addresses you select have access to your network.

Update all patches on servers and operating systems. Invest in regularly scheduled security audits or port scans to identify network vulnerabilities. PayPal Fraud Protection Services offers a free network scan from Qualys, included with every Basic or Advanced PayPal Fraud Protection Service.

Monitor firewall activity. Enterprise e-commerce companies should also monitor their network’s perimeter security on a 24-hour basis.

What Banks and Card Associations Are Doing to Prevent Online Credit Card Fraud

Consumers shop online for convenience and speed, but historical authentication requirements have often proved to be cumbersome, time-consuming, and ineffective.

New buyer authentication programs, such as MasterCard® SecureCode, and Verified by Visa®, provide more streamlined and customer-friendly authentication through passwords. These programs enable you to gain liability protection by prompting consumers to provide a password with their card issuers at checkout, similar to providing a PIN number for ATM transactions. Transactions in which consumers authenticate themselves to issuers effectively shift liability from the merchant to the issuer. Merchants are not held liable for fraudulent transactions processed using buyer authentication.

PayPal’s suite of Fraud Protection Services makes it easy for you to take advantage of this powerful system. (Check with your internet merchant account provider directly to determine if

they have deployed buyer authentication.) Through Fraud Protection Services, one seamless integration gives you access to both Verified by Visa and MasterCard SecureCode with your PayPal gateway service.

What PayPal Is Doing to Protect Your Business Against Fraud

The security of your information, transactions, and money is the core of our business and our top priority at PayPal. We help you protect against fraud, so you can grow your business and minimize losses.

PayPal leverages the Secure Sockets Layer (SSL) protocol, which provides crucial online identity and security to help establish trust between parties involved in e-commerce transactions. Customers can be assured that the website they're communicating with is genuine and that the information they send through web browsers stays private and confidential.

Moreover, using SSL with an encryption key length of 128 bits (the highest level commercially available), PayPal automatically encrypts your confidential information in transit from your computer to ours. Once your information reaches us, it resides on a server that is heavily guarded both physically and electronically. Our servers sit behind a monitored electronic firewall and are not connected directly to the internet, so your private information is available only to authorized computers.

How to Reduce Chargebacks

Dealing effectively with customer issues is a great way to minimize risk and reduce chargebacks. By communicating clearly and keeping good records, you can avoid many potential problems today, which are much easier than trying to resolve them with a credit card company tomorrow. PayPal has developed these helpful tips for avoiding customer complaints that can lead to chargebacks:

- Provide realistic delivery time estimates and use tracking that shows proof that the items were received
- Describe the sale item in as much detail as possible. Include clear images and measurements so that customers have a good understanding of what they're getting.
- Make sure you clearly disclose the total cost to customers up front: the price, taxes, shipping costs, etc.
- Provide customers with a way to contact you should they have a problem. Often a simple email exchange or phone call clears up a misunderstanding instantly.
- Respond promptly and courteously to customer inquiries.

Disclosure and Compliance

Disclosure Policy

Your disclosure policy tells your customers that you're honest and dependable and that you care about them and protecting their information. It shows your customers that you believe in transparency and accountability. It provides a framework and standards for your business policies, how you deal with your customer information, and how you communicate with your customers.

Your disclosure policy typically includes five things: a business description, privacy policy, shipping policy, return policy, and contact information. The more your customers know about you, the more comfortable they'll be giving you their business. So be honest, open, direct, and precise. Here are more details about the five areas you should cover:

- 1. Business description.** Write a clear description of what your company does, including what products and services it provides. Post it in a prominent place on your website, often the "About Us" section.
- 2. Privacy policy.** Your privacy policy should clearly state how you treat and protect your customers' information. It's essential that your policy is easy to find on your website, usually linked from your homepage. Typical elements of a privacy policy include:
 - What personally identifiable customer information you collect
 - How the information is used
 - With whom you share and do not share this information
 - What choices are available to your customers regarding collection, use, and distribution of the information
 - What choices are available to your customers regarding communications from you – email, direct mail, etc.
 - The kind of security procedures in place to protect the loss, misuse, or alteration of information under your control
 - How your customers can correct any inaccuracies in the information
- 3. Shipping policy.** You've made the sale. Your customers are anxious to get their purchases. So keep that excitement and positive momentum going with a shipping policy that's simple and straightforward:
 - Spell out your shipping terms in detail, disclosing if costs are determined by weight or the amount of the purchase
 - Indicate the classes of shipping you offer - ground, express, overnight, etc.
 - Indicate if you ship to APO, FPO, and international addresses
 - Tell your customers in what timeframe they can expect their purchase
 - Show your customers how they can track their shipment. (Your shippers should be able to provide most of this information for you.)

- 4. Return policy.** Your customers love simplicity and forgiveness. They sometimes make mistakes and order the wrong products. They may be unfamiliar with what they are ordering, and it's not what they had in mind. By allowing your customers to return an item in a timely fashion, and making it easy to do so, you are gaining their loyalty. A clear return policy also comes in handy if the order arrives damaged. So make it easy for them to initiate returns:
- Spell out exactly what your return policy is, for example that you accept returns only as exchanges or you accept returns and will credit their payment card
 - Be specific about how many days after purchase the item can be returned in order to get a credit or exchange
 - Let them know if you charge a restocking fee on returns
 - Include a return shipping label with every order
 - Provide clear return instructions, such as asking for a reason for the return and a telephone number in case you have questions
 - Provide guidance on how to pack the return and where they should bring it to ship it back to you
 - Include your customer service number or email address in case customers have questions or comments.
- 5. Contact information.** Keep the channels of communication open. Make it easy for your customers to get in touch with you:
- Give examples of reasons they may want to contact you, for example questions about privacy policy, return policy, availability of goods, etc.
 - Provide a phone number, and give the days and hours the phone lines are answered
 - Provide an email address, and give a timeframe when an answer can be expected
 - Provide a mailing address, and suggest to whose attention it should be addressed

PCI Data Security Standard Compliance

Just as a disclosure policy describes your business and states your business practices, your compliance with the PCI Data Security Standard communicates how much you care about your customers and reinforces an atmosphere of safety for all online merchants.

Consumers are becoming increasingly aware of the dangers of identity theft due to compromised data and stolen credit card information. PCI compliance assures your customers that you're looking out for their safety and well-being. Approach it with that in mind, and you transform compliance into a competitive edge and asset instead of a dreaded "must do."

Today, virtually all major credit card companies, including American Express®, Diners Club®, Discover® Card, JCB®, MasterCard International®, and Visa® U.S.A., require merchants and service providers to comply with the PCI standard. When you process credit card transactions through a merchant account, you also need to meet PCI validation requirements, including quarterly and annual audits, security self-assessments, and security scans. Your exact validation requirements are determined by your volume of credit card transactions.

While validating that you're in compliance with the PCI standard is a requirement, it's also an opportunity. Finding and fixing compliance gaps before your audit keeps your company running smoothly and your reputation intact. It provides you with tangible proof that you can communicate to your customers on how well you're protecting them.

The quickest and easiest way to meet PCI compliance standards is to outsource the job. A number of PayPal payment solutions are hosted, relieving the online merchant of the compliance responsibility. The PayPal Gateway payment solution, which allows the merchant to handle credit data, does require compliance and validation by the merchants themselves.

TABLE 2.2 PCI Data Security Standard

Standards	Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored data. 4. Encrypt transmission of cardholder data and sensitive information across public networks.
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update antivirus software. 6. Develop and maintain secure systems and applications.
Implement Strong-Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security.

The compliance level of each merchant is the responsibility of the merchant's acquiring bank (a bank that provides credit card merchant accounts and is responsible for submitting credit card purchase information to the credit card associations). The four merchant levels are based on annual credit card transaction volume.

TABLE 2.3 Merchant Levels for PCI Compliance

Level	Description
Level 1	<p>Any merchant – regardless of acceptance channel – processing over 6 million credit card transactions per year.</p> <p>Any merchant that has suffered a hack or an attack that resulted in an account data compromise.</p> <p>Any merchant identified by any card association as Level 1.</p>
Level 2	Any merchant processing 150,000 to 6 million e-commerce transactions per year.
Level 3	Any merchant processing 20,000 to 150,000 e-commerce transactions per year.

TABLE 2.3 Merchant Levels for PCI Compliance

Level	Description
Level 4	Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants processing up to 6,000,000 credit card transactions per year.

In addition to adhering to the PCI Data Security Standard, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and may be required for Level 4 merchants.

TABLE 2.4 PCI Compliance Validation Requirements

Level	Validation Action	Validated By
Level 1	Annual Onsite PCI Data Security Assessment and Quarterly Network Scan	Qualified Data Security Company or Internal Audit if signed by Officer of the company Qualified Independent Scan Vendor
Level 2 and 3	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	Merchant Qualified Independent Scan Vendor
Level 4	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	Merchant Qualified Independent Scan Vendor

NOTE: Level 4 merchants must comply with the PCI Data Security Standard. However, compliance validation for merchants in this category is determined by the merchant's acquirer.

Additional Resources About Disclosure and Compliance

There are other online resources that can help you in developing your own disclosure policy and meeting PCI compliance requirements. They include:

- The Privacy Planner from BBBOOnline helps you create a simple, solid, online privacy policy for your e-commerce business: <http://www.privacyplanner.com>.
- The Direct Marketing Association (DMA) offers a small businessfriendly online privacy policy generator: <http://www.the-dma.org/privacy/privacypolicygenerator.shtml>.
- The Federal Trade Commission offers valuable information on preventing identity theft at <http://www.consumer.gov/idtheft/>. Also be sure to visit the central FTC site at <http://www.ftc.gov/> for additional information and advice.
- Both the Visa and MasterCard websites have extensive information about meeting PCI Payment Data Security Standards: <http://www.visa.com> and <http://www.mastercard.com>.

PayPal Fraud Protection Services

Protecting your business against the consequences of even a single fraud attempt requires a significant time commitment and ties up valuable resources. PayPal has designed its suite of Fraud Protection Services based on merchant feedback and the needs of the online business community. Our solution not only gives you added protection against credit card fraud, cash fraud, and hacking attempts, but it also allows you to manage all these features quickly and easily with a single, intuitive interface.

Each PayPal Payflow Gateway solution includes standard antifraud features:

- **Card security code.** A three- or four-digit number printed on the physical card, which a customer provides to you at checkout.
- **Address verification system (AVS).** A system that verifies the credit card holder's personal address and billing information.

Each Fraud Protection service also offers a Buyer Authentication upgrade option that seamlessly integrates an advanced antifraud feature that allows credit card holders to submit a special password directly to their card-issuing bank during a transaction. Buyer Authentication provides essential merchant liability protection against fraudulent credit card transactions.

TABLE 2.5 Fraud Protection Services Purchase Options

Service	Merchant Type	Key Benefits
Package Options		
Basic	Designed for merchants with low transaction volume	Maximum ease and convenience
Advanced	Designed for merchants with mid- to high-level transaction volumes	Maximum customization and protection
Upgrade Options		
Account Monitoring	All merchants	Account activity monitoring seven days a week
Buyer Authentication	All merchants	Card association liability protection for authenticated shoppers

Detailed Service Descriptions

Basic Fraud Protection Service

Basic Fraud Protection Service is the ideal solution for merchants who process low transaction volumes through a Payflow payment gateway. It offers industry-leading security technology at an affordable price and lets your business:

- **Maximize liability protection.** Meet credit card company standards for address verification and card security codes.

- **Reduce chargeback costs.** Automatically reject or flag transactions that you deem suspicious.
- **Get started fast.** Quickly set up and manage your security system with easy-to-use tools.

Basic Fraud Protection Service works by using:

- **Filters.** Quickly set up filters that you can customize to fit your business needs.
- **Online reports.** Easily review and then accept or reject online orders.
- **Monitoring.** Standard reports let you check on filter and their effects.

Advanced Fraud Protection Service

Advanced Fraud Protection Service is essential for businesses processing medium-to-high transaction volumes, handling international customers, or selling high-risk merchandise through a Payflow payment gateway. It is a flexible security solution that helps your business:

- **Avoid losses.** Special tools flag unusual orders, questionable addresses, high-risk payments, and international orders.
- **Lower costs.** Spend less money on fraud management by automating order reviews and tailoring the system to meet your needs.

Advanced Fraud Protection Service works by using:

- **Enhanced filters.** Supplement the basic filters with ones specially suited for your high-risk needs.
- **Online reports.** Easily accept or reject online orders with the added security benefit of audit reports.
- **Watch lists.** Create custom lists based on products or other criteria.
- **Trusted transaction lists.** Establish lists that accept or deny transactions based on bad emails or credit cards.
- **Full testing.** Test your system before going live to determine its effect on your business and customers.

TABLE 2.6 Comparison of Fraud Protection Services

Features	Basic Protection	Advanced Protection
PayPal Fraud Manager Take control: find suspicious transactions with transaction review module, resolve chargebacks using audit trails, and tune filters to your business needs.	X	X
Unusual Order Filters Catch common fraud warnings like high dollar amounts, high quantities, and shipping/billing address mismatch.	X	X
High-Risk Payment Filters Catch suspicious transactions like rapid repeat buying from an internet address.	X	X

TABLE 2.6 Comparison of Fraud Protection Services

Features	Basic Protection	Advanced Protection
High-Risk Address Filters Check for suspect zip codes and freight forwarders plus IP address.	X	X
Automatic Rejection Lists Help protect you business from known offenders.		X
Automatic Acceptance Lists Keep good customers buying by automatically accepting their payments.		X
High-Risk International Filters Identify risky international payments.		X
Additional Risk Filters Get more tools to catch warning signs like rapid card use, risky banks, and tighter address validations.		X
Custom Filter Wizard Customize new rules that match your specific business needs.		X
Operations Security Identify vulnerabilities and list fixes with a security audit from Qualys.	X	X

PayPal Fraud Protection Services Upgrade Options

Account Monitoring

The Account Monitoring service uses trained security professionals who constantly monitor your business for suspicious activities and take action to protect it. Account Monitoring provides:

- **Security.** Our full-time protection keeps an eye on suspicious activity related to credits and refunds.
- **Assistance.** Our security professionals help prevent fraud by blocking settlements of suspicious transactions. If loss occurs, we work with law enforcement and your bank to assist in recovery.
- **Prevention.** We give customized recommendations to avoid future fraud.
- **Ease of use.** No lengthy set-up or configuration process.

Buyer Authentication

Buyer Authentication provides the Verified by Visa and MasterCard SecureCode. By adding Buyer Authentication to your Basic or Advanced Fraud Protection Service, your business receives merchant liability protection on qualified credit card transactions. Buyer Authentication gives you:

- **Single pre-integrated solution.** Add Buyer Authentication and take full advantage of both services without wasting staff and infrastructure resources integrating them yourself.

- **Extra security measure.** At checkout, customers are required to enter a password to verify their identity with their credit card company.
- **Maximum protection.** Once the cardholder's password is authenticated, Visa and MasterCard cover the merchant's liability for that transaction.

Review Questions

Answers to review questions are in [Appendix A, "Answers to Review Questions."](#)

1. Indicate if each statement is True (T) or False (F).

_____ Every merchant is at risk for fraud.

_____ Internet fraud is as easy to detect as in the brick-and-mortar world.

_____ Credit card associations hold merchants liable for fraudulent transactions because the credit card is not physically present during online purchases.

_____ American Express, Diners Club, Discover Card, JCB, MasterCard International, and Visa U.S.A. have adopted the Payment Card Industry (PCI) Data Security Standard developed to protect account and transaction information of cardholders.

_____ According to Gartner Group estimates, merchants reject an estimated 2% of all transactions out of suspicion of fraud, while in reality, 5% of transactions are actually fraudulent.

2. List the four most common fraud-related risks facing online merchants.

— _____

— _____

— _____

— _____

3. Match each participant in the payment processing network to the role they perform.

Response	Risk Category	Potential Risk Description
	Merchants with vulnerable security defenses	1. Fraud attempts are higher for merchants who advertise heavily or are in the news because criminals know that merchants who experience high transaction volumes have less time to defend against fraud.
	High-visibility merchants	2. It is difficult to validate the address or identity of foreign buyers, and it is more difficult to investigate and prosecute fraudulent activity from an overseas source.
	High-ticket goods that are easily resold	3. These items, including luxury goods, computers, and other electronic equipment, are most attractive to criminals.
	Goods that can be downloaded from the internet	4. Criminals know that you have limited time for fraud protection when sales volumes are high. That's why internet fraud triples in the fourth quarter.
	International customer base	5. Criminals watch for special offers. They know that you have limited time for fraud protection measures when sales volumes are high.
	Heavy proportion of fourth quarter sales	6. The purchase of these goods doesn't require physical address information, making it easier for criminals to disguise a fraudulent transaction.
	Special promotions	7. Criminals take advantage of sophisticated spidering techniques to identify merchants with network vulnerabilities, and can then break into your network to steal account access information for hijacking or merchant takeovers.

4. List two actions you can take to ensure that each transaction your website accepts and processes is valid.

— _____

— _____

5. Fill in the blanks to complete the following statements.

PayPal leverages the _____, which provides crucial online identity and security to help establish trust between parties involved in e-commerce transactions.

Using SSL with an encryption key length of _____ (the highest level commercially available), PayPal automatically encrypts your confidential information in transit from your computer to ours.

PayPal's servers sit behind a monitored _____ and are not connected directly to the internet, so your private information is available only to authorized computers.

6. List three ways to reduce chargebacks.

— _____

— _____

— _____

7. List the five areas you should cover in your website disclosure policy.

— _____

— _____

— _____

8. The left column in the table lists the PCI data security standards. The right column contains a list of requirements. Indicate which requirements meet each standard. (Note: Each standard has one or more requirements.)

Response	Standards	Requirements
	Build and Maintain a Secure Network	1. Restrict physical access to cardholder data. 2. Regularly test security systems and processes. 3. Develop and maintain secure systems and applications. 4. Encrypt transmission of cardholder data and sensitive information across public networks. 5. Protect stored data. 6. Assign a unique ID to each person with computer access. 7. Use and regularly update antivirus software. 8. Do not use vendor-supplied defaults for system passwords and other security parameters. 9. Track and monitor all access to network resources and cardholder data. 10. Maintain a policy that addresses information security. 11. Install and maintain a firewall configuration to protect data. 12. Restrict access to data by business need-to-know.
	Protect Cardholder Data	
	Maintain a Vulnerability Management Program	
	Implement Strong-Access Control Measures	
	Regularly Monitor and Test Networks	
	Maintain an Information Security Policy	

9. Define the following standard antifraud features included with each PayPal Payflow Gateway solution.

- Card security code

- Address verification system (AVS).

10. Indicate if each statement is True (T) or False (F).

- _____ PayPal's Basic Fraud Protection Service is the ideal solution for merchants who process low transaction volumes through a Payflow payment gateway, while the Advanced Fraud Protection Service is essential for businesses processing medium-to-high transaction volumes.
- _____ Both the Basic Fraud Protection Service and the Advanced Fraud Protection Service catch common fraud warnings like high dollar amounts, high quantities, and shipping/billing address mismatch.
- _____ To support automatic rejection lists and automatic acceptance lists, you need to upgrade to PayPal's Advanced Fraud Protection Service.
- _____ The PayPal Basic Fraud Protection Service provides full-time protection to keep an eye on suspicious activity related to credits and refunds.

3

Getting Started With Account Setup

In this chapter, you will learn about:

- Steps for getting started with PayPal payment processing solutions
- Enrolling with PayPal services
- The PayPal Sandbox including how to get access to the Sandbox

Basic Steps for Getting Started

In three steps, you can acquire everything you need to begin accepting online purchases.

1. Choose payment processing services.

- Website Payments Pro
- Website Payments Standard
- Payflow Pro
- Payflow Link
- Email Payments
- Virtual Terminal

2. Set up an internet merchant account, if you don't already have one.

All online businesses need to operate with an internet merchant account, primarily for depositing and refunding online payments. Website Payments Pro and Standard feature an integrated internet merchant account and gateway to make it quick and easy for you to begin doing business online.

If you register for either Payflow Pro or Payflow Link and already have an internet merchant account, PayPal will provide you the option to apply for an internet merchant account with PayPal's preferred merchant account provider.

To set up an internet merchant account, go to: https://www.paypal.com/cgi-bin/webscr?cmd=_registration-run. Have the following information available:

- Account/business owner's name, address, and email
- Business name and address
- Customer service information

Allow up to three to five business days to complete the setup and approval.

3. Enroll in the selected PayPal services.

A merchant must enroll for each service they plan to use. Once you have a merchant internet account, you can sign up for each service individually. To apply for Website Payments Pro, follow these steps:

- Go to: https://www.paypal.com/cgi-bin/webscr?cmd=_wp-pro-overview-outside.
- At the bottom of the page, click Apply for Website Payments Pro.
- When prompted, sign in using your Email Address and PayPal Password.
- Complete the steps to enroll with Website Payments Pro. You will submit an application that includes business information and your social security number or employer identification number and accept the billing agreement.

4. Use the PayPal APIs to implement payment processing on the merchant website.

You should carefully design and plan each merchant website implementation and feature. Work with the website owner to define the application requirements and ensure that your application complies with PayPal standards. This guide describes PayPal standards as they apply to each component of a merchant application.

5. Customize your payment processing service with additional services.

Protect the business and customers from fraud:

- **Fraud Protection Services.** From simple automated credit card fraud screening to enterprise-grade perimeter security services, PayPal can save you time and money while protecting your business.
- **Express Checkout.** Provides your customers with a secure and convenient payment flow because they don't have to re-enter information already stored in their PayPal account.

Accept repeat payments from customers:

- **Recurring Billing Service.** A fast, cost-effective way to accept repeat payments for installment plans, monthly fees, or subscription-based services.

Offer customers an alternative to credit card payments. Providing customers with a variety of payment choices, including credit cards and PayPal, has been shown in several industry studies to contribute to an increase in revenue.

For More Information. For additional PayPal product and pricing information, call 1-888-847-2747, send an email to paymentsales@paypal.com, or visit the PayPal Merchant Services section of the PayPal website at www.paypal.com.

PayPal Sandbox

The *PayPal Sandbox* is a self-contained environment in which developers can prototype and test PayPal applications. Before moving any PayPal-based application into production, test the application in the Sandbox to ensure that it functions properly.

For details about the Sandbox, see [Chapter 9, “Sandbox Testing”](#).

Review Question

Answers to review questions are in [Appendix A, “Answers to Review Questions”](#).

- The following steps describe the getting started with account setup process. Indicate the correct order of the steps by placing the step number to the left of each description.

- _____ Set up an internet merchant account, if you don't already have one.
- _____ Customize your payment processing service with additional services.
- _____ Choose payment processing services.
- _____ Use the PayPal APIs to implement payment processing on the merchant website.
- _____ Enroll in the selected PayPal services.

- What information do you need to set up an internet merchant account?

- How many days should you allow to set up an internet merchant account?

- Match each PayPal service that provides fraud protection to its description.

Response	PayPal Product	Service Description
	Fraud Protection Services	1. Provides your customers with a secure and convenient payment flow because they don't have to re-enter information already stored in their PayPal account.
	Express Checkout	2. A fast, cost-effective way to accept repeat payments for installment plans, monthly fees, or subscription-based services.
	Recurring Billing Service	3. Provides simple automated credit card fraud screening to enterprise-grade perimeter security services to save you time and money while protecting your business.

5. What is the purpose of the PayPal Sandbox?

4

API Credentials

In this chapter, you will learn:

- What API credentials are
- How to establish API credentials
- How to use API credentials

What API Credentials Are

Before using the PayPal API to communicate with the API server, a developer must establish a set of *API credentials*, which is data that uniquely identifies a developer to the PayPal API server. The credentials are included with each API call. Credentials are needed per merchant account for processing.

API credentials comprise the following:

- **API username** — This is assigned by PayPal. Although the API username is based on the email address used to set up the credentials, it is *not* the same as the email address used to log in to the PayPal website.
- **API password** — This is automatically generated and assigned by PayPal. It is a randomly generated string of 16 characters.
- **API certificate or API signature** — An *API signature* is an encrypted string value included with each API call. An *API certificate* is a file (downloaded from PayPal) that includes a key and certificate that identify a developer. An API certificate must be installed on a web server; therefore, it is an option only if the developer has full control of the web server.

Choosing an Authentication Method

Each authentication method (API signature and API certificate) has pros and cons. An API signature is easier and quicker to implement. An API certificate offers greater security.

PayPal recommends the use of an API signature, because of its greater simplicity; however, the PayPal API performs equally well with API signatures or API certificates.

Establishing API Credentials

The two authentication methods have separate processes for establishing API credentials.

API Signature

To establish credentials using an API signature as the authentication method, follow these steps:

1. Log in to a PayPal Premier or Business account.
2. In the top navigation area, click the **Profile** subtab.
3. Under the Account Information header, click the **API Access** link.
4. Click **Request API Credentials**.
5. Under **Credential Type**, click the **API Signature** radio button.
6. Click the agreement checkbox, and click **Submit**.
7. Record the API username and API password values.
8. The API signature is the Signature Hash value. Record this value, and store it in a document in a secure location.

The developer must take the appropriate steps to protect the API signature values; these values should be stored in a secure location on the web server.

To use the Sandbox to test an application, register a separate set of API credentials and use a second API signature. The same API signature cannot be used for both the Sandbox and live servers.

API Certificate

To establish credentials using an API certificate, follow these steps:

1. Generate the API certificate.
2. Encrypt the API certificate.
3. Install the API certificate in the Windows Certificate Store.

These steps are required regardless of whether the API certificate will be used with the PayPal Sandbox or with live PayPal. Each step is detailed below.

Generate the API Certificate

1. Log in to a PayPal Premier or Business account.
2. In the top navigation area, click the **Profile** subtab.
3. Under the **Account Information** header, click the **API Access** link.
4. Click the **Request API Credentials** link.
5. Complete the request form by clicking the agreement checkbox and clicking **Submit**.
6. Save the values for API Username and API Password.
7. Click the **Download Certificate** button. A file named `cert_key_pem.txt` is downloaded; this is the live API certificate.
8. Rename the file to something more meaningful, such as `paypal_live_cert.pem` (it is not necessary to keep the `.txt` suffix). This will differentiate a live API certificate from one used in the PayPal Sandbox.

Encrypt the API Certificate

NOTE: This step is required only with the PayPal SDK for Java, .NET, or Classic ASP.

1. Install the OpenSSL encryption tool on the system where the encryption will be performed. Make sure to include OpenSSL in the system's `PATH` variable.
2. Open a command prompt.
3. Go to the directory that contains the certificate to be encrypted.
4. Execute the following command:

```
openssl pkcs12 -export -in cert_key_pem.txt -inkey certificateName
-out paypal_cert.p12
```

where *certificateName* is the name of the API certificate to be encrypted.

5. When prompted, enter an encryption password. This is the Private Key Password.
6. The encryption creates a file named `paypal_cert.p12`. Rename this file to something more meaningful, and note the file location. This is the encrypted API certificate.

Install the API Certificate

NOTE: This step is required only with the PayPal SDK for .NET or Classic ASP.

To use the API certificate with the .NET platform, the certificate must be imported into the Windows Certificate Store. This is a Windows requirement, not a PayPal requirement.

To import the API certificate into the Windows Certificate Store, use the Windows HTTP Services Certificate Configuration Tool, or `WinHttpCertCfg.exe`. This tool is freely available as part of the Windows Server 2003 Resource Kit.

To import the API certificate, execute the following command at a command prompt:

```
WinHttpCertCfg -i encryptedCertificateName -p privateKeyPassword
                -c LOCAL_MACHINE\my -a username
```

where:

- *encryptedCertificateName* is the name of the encrypted API certificate that was generated with OpenSSL.
- *privateKeyPassword* is the private key password of the encrypted API certificate.
- *username* is the name of the user executing the application.

If the API certificate will be used with the PayPal Sandbox, set *username* to `Everyone`. Do not use `Everyone` with a live API certificate, because granting private-key access to all users on the server is not secure.

For an ASP.NET application, this value is `ASPNET`.

Under Windows IIS 5 (default configuration), this value is `IWAM_machineName`, where *machineName* is the appropriate computer name.

Under Windows IIS 6 (default configuration), this value is `"NETWORK SERVICE"` (including the quotation marks).

Using API Credentials

Each request to the PayPal server must include a set of required security parameters, shown in [Table 4.1](#).

TABLE 4.1 Required Security Parameters

Parameter	Required/Optional	Value
USER	Required	The API username.
PWD	Required	The API password.
VERSION	Required	The version number of the NVP API service. As of this printing, this value must be 3.3. Future versions of the NVP API service will require different values.
SIGNATURE	Optional (only if using API signature authentication)	The API signature string. Do not include this parameter if an API certificate is being used.
SUBJECT	Optional (only if making a third-party API call)	The email address of the PayPal account that has granted permission to make the API call. Do not use this parameter for requests that are not third-party API calls.

IMPORTANT: In the final implementation, protect the values for USER, PWD, and SIGNATURE. The values should be stored in a secure location, with file permissions set so that only the system user who executes the web application can access it.

NOTE: To find the latest version number, go to www.paypal.com/IntegrationCenter.

Review Questions

Answers to review questions are in [Appendix A, “Answers to Review Questions.”](#)

1. True or false: API credentials must be included with only the first request sent to the PayPal server during each session.
2. True or false: The API username is separate from the email address used to access PayPal.

5

Name-Value Pair (NVP) API

In this chapter, you will learn:

- The basic steps for using the PayPal Name-Value Pair (NVP) API to integrate an application with PayPal
- How to communicate with the PayPal server using the request/response model and secure HTTP

Integrating with the PayPal API

The NVP API is a simple, programmatic interface that allows merchants to access the PayPal API.

The NVP API makes it easy to integrate PayPal with a web. Simply construct an NVP string and post it to the PayPal server using HTTPS. PayPal posts back a response in NVP format.

To get started with the PayPal NVP API, see the samples at https://www.paypal.com/IntegrationCenter/ic_nvp.html. An application can use the samples to send API calls to the PayPal Sandbox test environment. The web samples are documented in *PayPal Name-Value Pair API Developer Guide and Reference*.

Basic Steps

This section describes the basic steps for programming with the NVP API.

Create a Web Application

The NVP API implementation usually runs in a web application. You can write a new application from scratch or use one of the samples as a starting point.

Get API Credentials

To access the API, API credentials are needed for identification (either an API signature or API certificate).

For more information on API credentials, see “API Credentials” on page 47.

Create and Post the Request

Create an NVP request string, and post it to the PayPal server. Add code to the web application to do the following tasks:

1. Encode the name and value parameters in the request, to ensure the correct transmission of all characters. This is described in [“URL Encoding” on page 55](#).
2. Construct the NVP API request string, as described in [“NVP Format” on page 54](#) and [“Request Format” on page 56](#).
3. Post the NVP request to the PayPal server, as described in [“Posting Using HTTPS” on page 58](#).

Interpret the Response

PayPal processes the request and posts back a response in NVP format. Add code to the web application to do the following tasks:

1. Decode the name and value parameters in the response.
2. Parse the NVP API response string, as described in [“NVP Format” on page 54](#) and [“Response Format” on page 57](#).
3. Take appropriate actions based on successful and failed responses.

Technical Details

This section describes details of the technologies used by the NVP API.

Request-Response Model

When using the NVP API, the application posts a request to PayPal, and PayPal returns a response.

URL Format

The request and response are in URL-encoded format, which is defined by the Worldwide Web Consortium (W3C). URL is defined as part of the URI specification.

NVP Format

NVP is a way of specifying name-value pairs in a string.

An NVP string conforms to the following guidelines:

- The name is separated from the value by an equals sign (=); for example:
`FIRSTNAME=Robert`
- Name-value pairs are separated by an ampersand (&); for example:
`FIRSTNAME=Robert&MIDDLENAME=Herbert&LASTNAME=Moore`
- The NVP string is URL-encoded.

URL Encoding

You must URL encode the values included in each API request. The values in all API responses are also URL encoded. URL encoding ensures the proper transmission of special characters, characters that are not allowed in a URL, and characters that have special meaning in a URL, such as the equal sign and ampersand. For example, notice the following NVP string:

```
NAME=Robert Moore&COMPANY=R. H. Moore & Associates
```

The NVP string is URL-encoded as follows:

```
NAME=Robert+Moore&COMPANY=R%2E+H%2E+Moore+%26+Associates
```

Use the methods listed in [Table 5.1](#) to URL-encode or URL-decode NVP strings.

TABLE 5.1 URL-Encoding Methods

Language	Encode/ Decode	Method
ASP.NET	Encode	<code>System.Web.HttpUtility.UrlEncode (buffer, Encoding.Default)</code>
	Decode	<code>System.Web.HttpUtility.UrlDecode (buffer, Encoding.Default)</code>
Classic ASP	Encode	<code>Server.URLEncode</code>
	Decode	No built-in function
ColdFusion	Encode	<code>URLEncodedFormatstring [, charset]</code>
	Decode	<code>URLDecodeurlEncodedString[, charset]</code>
Java	Encode	<code>java.net.URLEncoder.encode</code>
	Decode	<code>java.net.URLEncoder.decode</code>
PHP	Encode	<code>urlencode ()</code>
	Decode	<code>urldecode ()</code>

Request Format

Each NVP request consists of required and optional parameters and their values. Parameter names are not case-sensitive. As shown in [Table 5.2](#), this document uses UPPERCASE for parameter names and divides the parameters into required security parameters and body parameters.

TABLE 5.2 General Format of a Request

Required security parameters	<p>USER=apiUsername&PWD=apiPassword&SIGNATURE=apiSignature&SUBJECT=optionalThirdPartyEmailAddress&VERSION=3.3</p> <p>The following parameters are always required:</p> <ul style="list-style-type: none"> • USER • PWD • VERSION=3.3 • SIGNATURE <p>NOTE: In the examples in this and other PayPal documents, the required security parameters sometimes appear like this:</p> <p>[requiredSecurityParameters]</p>
Body parameters	&METHOD=methodName&otherRequiredAndOptionalParameters

In practice, concatenate all parameter names and URL-encoded values in a single string. After the METHOD parameter, the parameters can be specified in any order.

Required Security Parameters

The required security parameters are the same as the developer's PayPal API credentials, which are described in [“API Credentials” on page 47](#).

API Parameters

The request body must contain the name of the API method in the METHOD parameter. In addition, each method has required and optional parameters:

METHOD=methodName&requiredAndOptionalParameters

All API methods and their parameters are detailed in *PayPal Name-Value Pair API Developer Guide and Reference*.

Response Format

A response from the PayPal servers is a URL-encoded name-value pair string, just like the request. The general format of the response is described in [Table 5.3](#).

TABLE 5.3 General Format of a Successful Response

Success response fields	ACK=Success&TIMESTAMP=date/timeOfResponse&CORRELATIONID=debuggingTokens&VERSION=3.3&BUILD=buildNumber
	NOTE: In the examples in this and other PayPal documents, the successful response header fields sometimes appear like this: [successResponseFields]
API response fields	&NAME1=value1&NAME2=value2...

Each response includes the ACK field. If the ACK field's value is `Success` or `SuccessWithWarning`, the application should process the API response fields. In a successful response, the application can ignore all fields up to and including `BUILD`; the important fields begin after `BUILD`.

The possible successful response fields for each method are detailed in the reference information for the API. How the application handles the fields depends on the particular API method called (such as filling in a form, updating a database, and so on).

ACK Parameter Values

[Table 5.4](#) lists the possible values for the ACK parameter.

TABLE 5.4 ACK Parameter Values

Type of Response	Value
Successful response	Success
	SuccessWithWarning
Error response	Error

Error Responses

If the ACK value is `Error`, the API response fields are not returned. The general format of an error response is described in [Table 5.5](#).

TABLE 5.5 Format of an Error Response

Response fields on error	ACK=Error&TIMESTAMP=date/timeOfResponse&CORRELATIONID=debuggingToken&VERSION=3.3&BUILD=buildNumber&L_ERRORCODE0=errorCode&L_SHORTMESSAGE0=shortMessage&L_LONGMESSAGE0=longMessage&L_SEVERITYCODE0=severityCode
--------------------------	--

Multiple errors can be returned. Each set of errors has a different numeric suffix, starting with 0 and incrementing by 1 for each error.

For possible causes of errors and how to correct them, see the error-message reference information in *PayPal Name-Value Pair API Developer Guide and Reference*.

Posting Using HTTPS

The web application posts the URL-encoded NVP string over an HTTPS connection to one of the PayPal API servers. PayPal provides a live server. It also provides a Sandbox server that allows applications to process transactions in a test environment.

API Servers for API Signature Security

If the application uses an API signature, post requests to one of the following servers:

- **Sandbox** — <https://api-3t.sandbox.paypal.com/nvp>
- **Live** — <https://api-3t.paypal.com/nvp>

API Servers for API Certificate Security

If the application uses an API certificate, post requests to one of the following servers:

- **Sandbox** — <https://api.sandbox.paypal.com/nvp>
- **Live** — <https://api.paypal.com/nvp>

Review Questions

Answers to review questions are in [Appendix A, “Answers to Review Questions.”](#)

1. What character is used to separate name/value pairs in an NVP string?
2. True or false: In an NVP request, parameter names are not case-sensitive.
3. In an NVP request, what parameter gives the name of the API call?
4. True or false: More than one error can be returned in a single error response.

6

Express Checkout

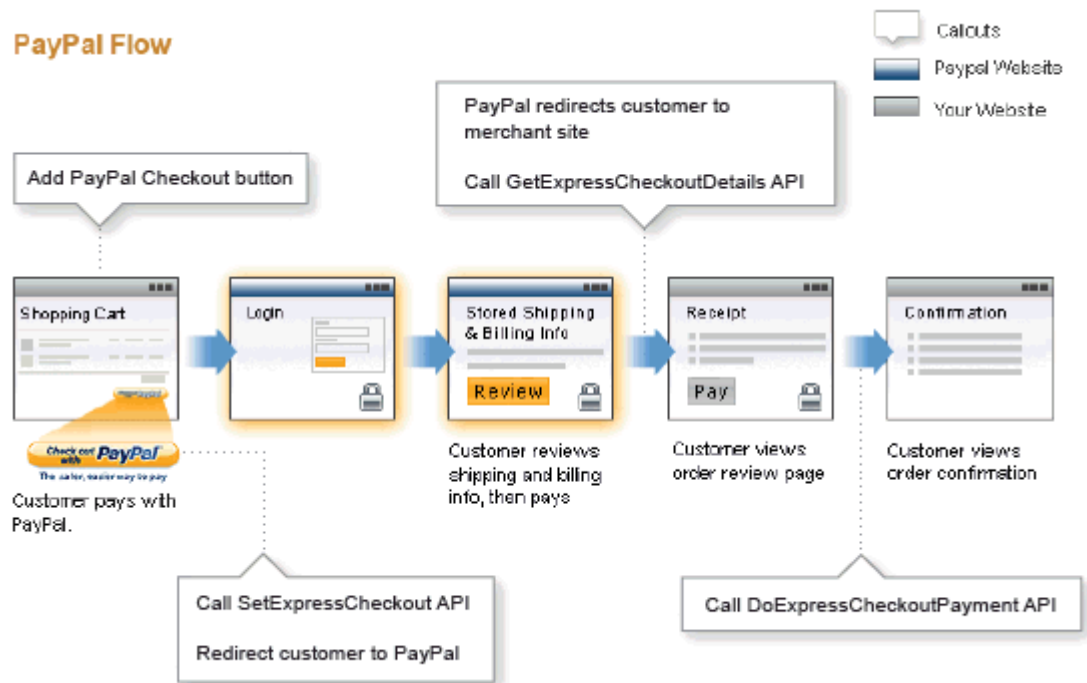
In this chapter you will learn:

- How Express Checkout works
- How to use the Express Checkout APIs
- How to use the PayPal Express Checkout buttons and logos

How Express Checkout Works

PayPal Express Checkout is a combination of the website checkout process, PayPal login and review pages on <https://www.paypal.com>, and PayPal API requests and responses. Express Checkout gives developers the flexibility to put PayPal either first in the checkout process or on the billing page along with other payment options. The customer always starts and completes an order on the merchant's website.

The following figure summarizes the Express Checkout work flow:



The PayPal Express Checkout API calls work as follows:

1. After selecting products to purchase, the customer clicks the **Checkout with PayPal** button on the merchant's website. This allows the customer to quickly skip entering shipping and billing information on the merchant's website.
2. The application passes PayPal the transaction details (`SetExpressCheckout`), receives the response from PayPal, and redirects the customer's browser to PayPal.
3. The customer logs in to PayPal.
4. The customer selects a shipping address and payment method stored on PayPal, and clicks **Continue Checkout** to approve the use of PayPal. PayPal redirects the customer to the merchant's website.
5. The application makes an API call to retrieve transaction details (`GetExpressCheckoutDetails`), and receives the response from PayPal.
6. The customer finishes the checkout process on the merchant's website, reviews the order, and completes the order. See [“Order Review Page Setup” on page 76](#) for recommendations on setting up an order-review page.

NOTE: The customer always reviews transaction details and makes the final payment on the merchant's website. PayPal handles the payment verification and passes the application the customer's shipping information. PayPal never shares the customer's financial information with anyone.

7. When the customer places the order, the application requests payment from PayPal (`DoExpressCheckoutPayment`). PayPal sends a response and sends the customer an email receipt for the payment.
8. The application transfers the customer to the order-confirmation page, showing the details of the transaction.

The PayPal Express Checkout program flow-of-control and integration points are summarized in [Table 6.1](#).

TABLE 6.1 Express Checkout Flow-of-Control and Integration Points

Customer...	Merchant...	PayPal...
Clicks Checkout with PayPal button.	Sends a <code>SetExpressCheckout</code> request with the required information—estimated <code>OrderTotal</code> , <code>ReturnURL</code> , and <code>CancelURL</code> —and optional fields, such as <code>MaxAmount</code> .	
		Returns a <code>SetExpressCheckout</code> response with <code>Token</code> .
	Adds value of <code>Token</code> from response as a name-value pair, and redirects the user's browser to: <code>https://www.paypal.com/cgi-bin/webscr?cmd=_express-checkout&token=value</code>	

TABLE 6.1 Express Checkout Flow-of-Control and Integration Points (Continued)

Customer...	Merchant...	PayPal...
Logs in to PayPal, approves PayPal use, and clicks Continue or Pay.		Redirects user's browser to merchant's ReturnURL, with Token value appended.
	Optionally sends a <code>GetExpressCheckoutDetails</code> request with <code>Token</code> to retrieve customer's information.	Returns a <code>GetExpressCheckoutDetails</code> response with <code>PayerID</code> , email address, shipping address, confirmed or unconfirmed status or that shipping address, and other details.
	Renders page in customer's browser for the next step in checkout process, such as the "Order Review" page.	
Clicks Confirm Order button	Calls <code>DoExpressCheckoutPayment</code> API with the required elements <code>Token</code> , <code>OrderTotal</code> , <code>PaymentAction</code> , and <code>PayerID</code> returned by <code>GetExpressCheckoutDetails</code> response.	Returns payment info with important <code>TransactionID</code> value and other details about the payment.
	Displays final page.	

Express Checkout API Reference Information

The following sections provide reference information about the parameters and fields used in the various requests and responses involved in PayPal Express Checkout.

Further reference information is available in *PayPal Name-Value Pair API Developer Guide and Reference*.

SetExpressCheckout Request

The `SetExpressCheckout` notifies PayPal that the application is using Express Checkout to obtain payment from the customer.

TABLE 6.2 *SetExpressCheckout Request Parameters*

Parameter	Description	Required?
METHOD	Name of the API: <code>SetExpressCheckout</code>	Yes
RETURNURL	<p>A secure URL to which the customer's browser is returned after the customer chooses to pay with PayPal.</p> <p>NOTE: PayPal recommends that the value be the final review page on which the customer confirms the order and payment.</p> <p>Character length and limitations: no limit.</p>	Yes
CANCELURL	<p>The URL to which the customer is returned if the customer does not approve the use of PayPal to pay the merchant.</p> <p>NOTE: PayPal recommends that the value be the final review page on which the customer confirms the order and payment.</p> <p>Character length and limitations: no limit.</p>	Yes
AMT	<p>The total cost of the order to the customer. If shipping cost and tax charges are known, include them in this value; otherwise, this value should be the current subtotal of the order.</p> <p>Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).</p>	Yes
CURRENCYCODE	<p>A three-character currency code for one of the PayPal-supported transactional currencies.</p> <p>Default value: USD</p>	No
MAXAMT	<p>The expected maximum total amount of the complete order, including shipping cost and tax charges.</p> <p>Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).</p>	No

TABLE 6.2 SetExpressCheckout Request Parameters (Continued)

Parameter	Description	Required?
PAYMENTACTION	<p>How the merchant wants to obtain payment:</p> <ul style="list-style-type: none"> • <code>Authorization</code> indicates this payment is a basic authorization subject to settlement with PayPal Authorization & Capture. • <code>Order</code> indicates this payment is an order authorization subject to settlement with PayPal Authorization & Capture. • <code>Sale</code> indicates this is a final sale for which the merchant is requesting payment. <p>NOTE: If this value is set to <code>Sale</code> on <code>SetExpressCheckoutRequest</code>, it cannot change to <code>Authorization</code> on the final <code>DoExpressCheckoutPaymentRequest</code>.</p> <p>Character length and limit: Up to 13 single-byte alphabetic characters. Default: <code>Sale</code></p>	No
EMAIL	<p>Email address of the customer as entered during checkout. PayPal uses this value to prefill the PayPal membership sign-up portion of the PayPal login page.</p> <p>Character length and limit: 127 single-byte alphanumeric characters</p>	No
DESC	<p>Description of items the customer is purchasing.</p> <p>Character length and limit: 127 single-byte alphanumeric characters</p>	No
CUSTOM	<p>A free-form field for the developer's own use, such as a tracking number or other value for PayPal to return in the <code>GetExpressCheckoutDetails</code> response and <code>DoExpressCheckoutPayment</code> response.</p> <p>Character length and limitations: 256 single-byte alphanumeric characters</p>	No
INVNUM	<p>The merchant's own unique invoice or tracking number. PayPal returns this value in the <code>DoExpressCheckoutPayment</code> response.</p> <p>Character length and limit: 127 single-byte alphanumeric characters</p>	No
REQCONFIRMSHIPPING	<p>The value <code>1</code> indicates that the merchant requires that the customer's shipping address on file with PayPal be a confirmed address.</p> <p>NOTE: Setting this field overrides the setting specified in the Merchant Account Profile.</p> <p>Character length and limitations: 1 single-byte numeric character. Allowable values: <code>0</code>, <code>1</code> Default value: <code>0</code></p>	No
NOSHIPPING	<p>The value <code>1</code> indicates that on the PayPal pages, no shipping address fields should be displayed whatsoever.</p> <p>Character length and limitations: 4 single-byte numeric characters. Allowable values: <code>0</code>, <code>1</code> Default value: <code>0</code></p>	No

TABLE 6.2 SetExpressCheckout Request Parameters (Continued)

Parameter	Description	Required?
ADDROVERRIDE	<p>The value 1 indicates that the PayPal pages should display the shipping address set in this <code>SetExpressCheckout</code> request, not the shipping address on file with PayPal for this customer.</p> <p>NOTE: Displaying the PayPal street address on file does not allow the customer to edit that address.</p> <p>Allowable values: 0, 1 Default value: 0</p>	No
TOKEN	<p>A timestamped token that tells PayPal that the payment is being processed with Express Checkout.</p> <p>NOTE: The token expires after three hours.</p> <p>If the token is set here, the value of <code>TOKEN</code> in the response will be identical to the value in the request.</p> <p>Character length and limitations: 20 single-byte characters</p>	No
LOCALECODE	<p>Locale of pages displayed by PayPal during Express Checkout.</p> <p>Character length and limitations: Any two-character country code.</p> <p>The following codes are supported by PayPal:</p> <ul style="list-style-type: none"> • AU • DE • ES • FR • GB • IT • US <p>All other values default to US.</p> <p>A complete list of country codes is in <i>PayPal Name-Value Pair API Developer Guide and Reference</i>.</p>	No
PAGESTYLE	<p>Sets the Custom Payment Page Style for payment pages associated with this button/link. This value corresponds to the HTML variable <code>page_style</code> for customizing payment pages. The value is the same as the Page Style Name chosen when adding or editing the page style from the Profile subtab of the My Account tab of the PayPal account.</p> <p>Character length and limitations: 30 single-byte alphabetic characters.</p>	No
HDRIMG	<p>A URL for the image to appear at the top left of the payment page. The image has a maximum size of 750 pixels wide by 90 pixels high. PayPal recommends that the image be stored on a secure (HTTPS) server.</p> <p>Character length and limit: 127 single-byte alphanumeric characters</p>	No

TABLE 6.2 SetExpressCheckout Request Parameters (Continued)

Parameter	Description	Required?
HDRBORDERCOLOR	Sets the border color around the header of the payment page. The border is a 2-pixel perimeter around the header space, which is 750 pixels wide by 90 pixels high. Character length and limitations: 6-character HTML hexadecimal color code in ASCII.	No
HDRBACKCOLOR	Sets the background color for the header of the payment page. Character length and limitations: 6-character HTML hexadecimal color code in ASCII.	No
PAYFLOWCOLOR	Sets the background color for the payment page. Character length and limitations: 6-character HTML hexadecimal color code in ASCII.	No
CHANNELTYPE	Type of channel: <ul style="list-style-type: none"> • Merchant — Non-auction seller • eBayItem — eBay auction 	No
SOLUTIONTYPE	Type of checkout flow: <ul style="list-style-type: none"> • Sole — Express Checkout for auctions • Mark — Normal Express Checkout 	No
Shipping Address	An optional shipping address, as described in “ ShippingAddress Parameter ” on page 153. ShippingAddress is optional, but if it is included, certain fields are required.	No

SetExpressCheckout Response

The SetExpressCheckout response is returned by the PayPal server after a SetExpressCheckout request is posted.

TABLE 6.3 SetExpressCheckout Response Fields

Parameter	Description
TOKEN	A timestamped token that tells PayPal that the payment is being processed with Express Checkout. NOTE: The token expires after three hours. If the token was set in the SetExpressCheckout request, the value of TOKEN in the response will be identical to the value in the request. Character length and limitations: 20 single-byte characters

GetExpressCheckoutDetails Request

A `GetExpressCheckoutDetails` request asks PayPal to respond with the customer's checkout information, such as shipping address.

TABLE 6.4 *GetExpressCheckoutDetails Request Parameters*

Parameter	Description	Required?
METHOD	Name of the API: <code>GetExpressCheckoutDetails</code>	Yes
TOKEN	A timestamped token, the value of which was returned by the <code>SetExpressCheckout</code> response. Character length and limitations: 20 single-byte characters. Allowable values: An unexpired token.	Yes

GetExpressCheckoutDetails Response

The `GetExpressCheckoutDetails` response provides the customer's checkout details, which were stored in the PayPal system.

TABLE 6.5 *GetExpressCheckoutDetails Response Fields*

Parameter	Description
TOKEN	The timestamped token value that was returned by the <code>SetExpressCheckout</code> response and passed in the <code>GetExpressCheckoutDetails</code> request. Character length and limitations: 20 single-byte characters.
EMAIL	Email address of payee. Character length and limitations: 127 single-byte characters.
PAYERID	Unique PayPal customer account identification number. Character length and limitations: 13 single-byte alphanumeric characters.
PAYERSTATUS	Status of payer. Character length and limitations: 10 single-byte alphabetic characters. Possible values: <code>verified</code> , <code>unverified</code>
SALUTATION	Payer's salutation. Character length and limitations: 20 single-byte characters.
FIRSTNAME	Payer's first name. Character length and limitations: 25 single-byte characters.
MIDDLENAME	Payer's middle name. Character length and limitations: 25 single-byte characters.
LASTNAME	Payer's last name. Character length and limitations: 25 single-byte characters.

TABLE 6.5 *GetExpressCheckoutDetails* Response Fields (Continued)

Parameter	Description
SUFFIX	Payer's suffix. Character length and limitations: 12 single-byte characters.
COUNTRYCODE	Payer's country of residence, in the form of ISO standard 3166 two-character country codes. Character length and limitations: 2 single-byte characters.
BUSINESS	Payer's business name. Character length and limitations: 127 single-byte characters.
SHIPTONAME	Person's name associated with this address. Character length and limitations: 32 single-byte characters.
SHIPTOSTREET	First street address. Character length and limitations: 100 single-byte characters.
SHIPTOSTREET2	Second street address. Character length and limitations: 100 single-byte characters.
SHIPTOCITY	Name of city. Character length and limitations: 40 single-byte characters.
SHIPTOSTATE	State or province. Character length and limitations: 40 single-byte characters.
SHIPTOCOUNTRYCODE	Country code. Character length and limitations: 2 single-byte characters.
SHIPTOZIP	US ZIP code or other country-specific postal code. Character length and limitations: 20 single-byte characters.
ADDRESSSTATUS	Status of street address on file with PayPal.
CUSTOM	A free-form field for the developer's own use, as set in the CUSTOM parameter of the SetExpressCheckout request. Character length and limitations: 256 single-byte characters.
INVNUM	The merchant's own invoice or tracking number, as set in the INVNUM parameter of the SetExpressCheckout request. Character length and limitations: 127 single-byte characters.
PHONENUM	Payer's contact telephone number. PayPal returns a contact telephone number only if the Merchant account profile settings require that the customer enter one. Character length and limitations: Field mask is XXX-XXX-XXXX (for U.S. numbers) or +XXX XXXXXXXX (for international numbers)

DoExpressCheckoutPayment Request

The `DoExpressCheckoutPayment` request performs the actual request to obtain payment with PayPal Express Checkout.

NOTE: PayPal requires that a merchant using Express Checkout display to the customer the same amount that the merchant sends to PayPal in the `AMT` parameter of the `DoExpressCheckoutPayment` request.

TABLE 6.6 *DoExpressCheckoutPayment Request Parameters*

Parameter	Description	Required?
METHOD	Name of the API: <code>DoExpressCheckoutPayment</code>	Yes
TOKEN	The timestamped token value that was returned by the <code>SetExpressCheckout</code> response and passed by the <code>GetExpressCheckoutDetails</code> request. Character length and limitation: 20 single-byte characters.	Yes
PAYMENTACTION	How the merchant wants to obtain payment: <ul style="list-style-type: none"> • <code>Authorization</code> indicates that this payment is a basic authorization subject to settlement with PayPal Authorization & Capture. • <code>Order</code> indicates that this payment is an order authorization subject to settlement with PayPal Authorization & Capture. • <code>Sale</code> indicates that this is a final sale for which the merchant is requesting payment. <p>NOTE: If this value was set to <code>Sale</code> on <code>SetExpressCheckoutRequest</code>, then it cannot change to <code>Authorization</code> on the final <code>DoExpressCheckoutPaymentRequest</code>.</p> Character length and limit: Up to 13 single-byte alphabetic characters. Default: <code>Sale</code>	Yes
PAYERID	Unique PayPal customer account identification number, as returned by the <code>GetExpressCheckoutDetails</code> response. Character length and limit: 13 single-byte alphabetic characters.	Yes
AMT	Total of order, including shipping, handling, and tax. NOTE: Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).	Yes

TABLE 6.6 DoExpressCheckoutPayment Request Parameters (Continued)

Parameter	Description	Required?
DESC	Description of items the customer is purchasing. Character length and limitations: 127 single-byte alphanumeric characters.	No
CUSTOM	A free-form field for the developer's own use. Character length and limitations: 256 single-byte alphanumeric characters.	No
INVNUM	The merchant's own invoice or tracking number. Character length and limitations: 127 single-byte alphanumeric characters.	No
BUTTONSOURCE	An identification code for use by third-party applications to identify transactions. Character length and limitations: 32 single-byte alphanumeric characters.	No
NOTIFYURL	The URL for receiving Instant Payment Notification (IPN) about this transaction. NOTE: If this value is not specified, the notification URL from the Merchant Profile is used, if one is available. Character length and limitations: 2,048 single-byte alphanumeric characters.	No
ITEMAMT	Sum of cost of all items in this order. NOTE: Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,). NOTE: ITEMAMT is required if a value is specified for L_AMTn.	No
SHIPPINGAMT	Total shipping costs for this order. NOTE: Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).	No
HANDLINGAMT	Total handling costs for this order. NOTE: Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).	No

TABLE 6.6 DoExpressCheckoutPayment Request Parameters (Continued)

Parameter	Description	Required?
TAXAMT	Sum of tax for all items in this order. NOTE: Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,). NOTE: TAXAMT is required if a value is specified for L_TAXAMT <i>n</i> .	No
CURRENCYCODE	A three-character currency code for one of the PayPal-supported transactional currencies. Default value: USD	No
L_NAME <i>n</i>	Item name. These parameters should be ordered sequentially, beginning with 0 (for example, L_NAME0, L_NAME1, and so forth). Character length and limitations: 127 single-byte characters.	No
L_NUMBER <i>n</i>	Item number. These parameters should be ordered sequentially, beginning with 0 (for example, L_NUMBER0, L_NUMBER1, and so forth). Character length and limitations: 127 single-byte characters.	No
L_QTY <i>n</i>	Item quantity. These parameters should be ordered sequentially, beginning with 0 (for example, L_QTY0, L_QTY1, and so forth). Character length and limitations: any positive integer.	No
L_TAXAMT <i>n</i>	Item sales tax. These parameters should be ordered sequentially, beginning with 0 (for example, L_TAXAMT0, L_TAXAMT1, and so forth). Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).	No
L_AMT <i>n</i>	Cost of item. These parameters should be ordered sequentially, beginning with 0 (for example, L_AMT0, L_AMT1, and so on). Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).	No
L_EBAYITEMNUMBER <i>n</i>	Auction item number. Character length: 765 single-byte characters.	No

TABLE 6.6 DoExpressCheckoutPayment Request Parameters (Continued)

Parameter	Description	Required?
L_EBAYITEMAUCTIONTXNID <i>n</i>	Auction transaction identification number. Character length: 255 single-byte characters.	No
L_EBAYITEMORDERID <i>n</i>	Auction order identification number. Character length: 64 single-byte characters.	No
ShippingAddress	An optional shipping address, as described in “ShippingAddress Parameter” on page 153 . ShippingAddress is optional, but if it is included, certain fields are required.	No

DoExpressCheckoutPayment Response

A DoExpressCheckoutPayment response is sent by the PayPal server after an Express Checkout transaction.

TABLE 6.7 DoExpressCheckoutPayment Response Fields

Field	Description
TOKEN	The timestamped token value that was returned by the SetExpressCheckout response and passed by the GetExpressCheckoutDetails request. Character length and limitation: 20 single-byte characters.
TRANSACTIONID	Unique transaction ID of the payment. NOTE: If the PaymentAction of the request was Authorization or Order, this value is the AuthorizationID for use with the Authorization & Capture APIs. Character length and limitations: 19 single-byte characters. Possible values: Transaction-specific
TRANSACTIONTYPE	The type of transaction. Character length and limitations: 15 single-byte characters Possible values: <ul style="list-style-type: none"> • cart • express-checkout
PAYMENTTYPE	Indicates whether the payment is instant or delayed. Character length and limitations: 7 single-byte characters Possible values: <ul style="list-style-type: none"> • none • echeck • instant
ORDERTIME	Time/date stamp of payment. Possible values: Transaction-specific

TABLE 6.7 DoExpressCheckoutPayment Response Fields (Continued)

Field	Description
AMT	The final amount charged, including any shipping and taxes from the Merchant Profile. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Regardless of currency, decimal separator is a period (.), and the optional thousands separator is a comma (.). Equivalent to 9 characters maximum for USD. Possible values: Transaction specific
CURRENCYCODE	A three-character currency code for one of the PayPal-supported transactional currencies. Default value: USD
FEEAMT	PayPal fee amount charged for the transaction. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Regardless of currency, decimal separator is a period (.), and the optional thousands separator is a comma (.). Equivalent to 9 characters maximum for USD. Possible values: Transaction-specific
SETTLEAMT	Amount deposited in the merchant's PayPal account after a currency conversion. Possible values: Transaction-specific
TAXAMT	Tax charged on the transaction. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Regardless of currency, decimal separator is a period (.), and the optional thousands separator is a comma (.). Equivalent to 9 characters maximum for USD. Possible values: Transaction-specific
EXCHANGERATE	Exchange rate if a currency conversion occurred. Relevant only if the merchant is billing in a currency other than the primary currency. If a conversion must occur, it occurs in the customer's account. Character length and limitations: A decimal that does not exceed 17 characters, including the decimal point Possible values: Transaction-specific
PAYMENTSTATUS	Status of the payment: <ul style="list-style-type: none"> Completed — The payment has been completed, and the funds have been added successfully to the merchant's account balance. Pending — The payment is pending. See the PENDINGREASON element for more information.

TABLE 6.7 DoExpressCheckoutPayment Response Fields (Continued)

Field	Description
PENDINGREASON	<p>The reason the payment is pending:</p> <ul style="list-style-type: none"> • none — No pending reason. • address — The payment is pending because the customer did not include a confirmed shipping address, and the merchant's Payment Receiving Preferences are set such that the payments must be manually accepted or denied. To change these preferences, the merchant must go to the Preferences section of the Profile. • echeck — The payment is pending because it was made by an eCheck that did not yet clear. • intl — The payment is pending because the merchant holds a non-US account and does not have a withdrawal mechanism. The merchant must manually accept or deny this payment from the Account Overview. • multi-currency — The merchant does not have a balance in the currency sent, and the merchant does not have the Payment Receiving Preferences set to automatically convert and accept this payment. The merchant must manually accept or deny this payment. • verify — The payment is pending because the merchant is not yet verified. The merchant must verify his account before accepting this payment. • other — The payment is pending for a reason other than those listed here. For more information, contact PayPal customer service.
REASONCODE	<p>The reason for a reversal, if the transaction type is reversal:</p> <ul style="list-style-type: none"> • none — No reason code. • chargeback — A reversal has occurred on this transaction due to a chargeback by the customer. • guarantee — A reversal has occurred on this transaction due to the customer triggering a money-back guarantee. • buyer-complaint — A reversal has occurred on this transaction due to a complaint about the transaction from the customer. • refund — A reversal has occurred on this transaction because the merchant gave the customer a refund. • other — A reversal has occurred on this transaction due to a reason not listed here.

Button and Logo Placement and Use

When you offer PayPal Express Checkout to customers, you are required to display the option in two places on your website:

1. As a checkout choice on the shopping-cart page, display the Express Checkout button as follows:
2. As a Payment Method on the billing page, display the PayPal acceptance mark as a payment option.

If your site requires customers to sign in or create a store account before checkout, the Express Checkout button should be visible before users are required to sign in.

If your site has a Checkout button on pages other than the Shopping Cart page (such as on product pages), PayPal requires that you put a PayPal Express Checkout button next to these Checkout buttons as well—if the Checkout button initiates the checkout flow. If the Checkout button links to the Shopping Cart page, you are not required to place a PayPal button.

The HTML for the Express Checkout button and PayPal Acceptance Mark are available at <https://www.paypal.com/express-checkout-buttons>.

PayPal Button as a Checkout Choice

The following figure shows PayPal as a checkout-choice button:

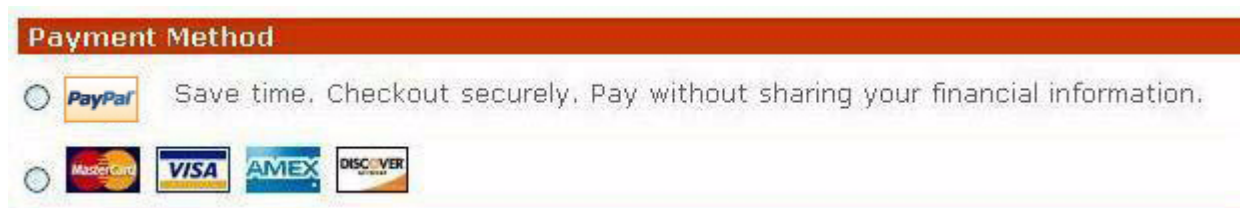


Place the Express Checkout button on the shopping-cart page, arranged as follows:

- Always clickable
- Right below or next to each of your own cart's checkout buttons (with the word "or" between them)
- Before your website collects any shipping or billing details or displays any other payment methods
- Aligned vertically or horizontally with your own buttons

PayPal Button as a Payment Method

The following figure shows PayPal as a payment method:



Display PayPal as the default payment option, selected next to the other payment options at the end of checkout.

When displaying PayPal with other payment options, PayPal highly recommends that you use radio buttons. If your website cannot accommodate radio buttons, you may use horizontal fields or an entry in a drop-down list.

Using PayPal-Hosted Images

PayPal requires that you use Express Checkout button images hosted on PayPal's secure servers, rather than hosting copies of these images on your own servers. Also, using the buttons on the PayPal servers eliminates the need for you to maintain them yourself. If the buttons are updated, the new buttons appear automatically in your application. Using out-of-date PayPal buttons could reduce customer confidence in your PayPal deployment.

When you get the HTML code at <https://www.paypal.com/express-checkout-buttons>, it will work only with PayPal-hosted buttons.

Tips

- Create checkout pages that are uncluttered and free from visual distractions.
- Keep the checkout flow to as few a number of pages as possible.
- Be sure that the PayPal Express Checkout button is clickable, and all PayPal buttons are used for the use they were intended.
- Do not use the Preview button when the next page is actually a purchase.
- Avoid using warning or legal text as part of the primary checkout experience.
- Do not alter, recolor, or resize the PayPal Express Checkout button, or adding text around the PayPal checkout button.

Redirecting to PayPal

After the response from `SetExpressCheckout`, the application must redirect the customer's browser to PayPal. The `SetExpressCheckout` response includes an Express Checkout session token. Add the value of the `Token` from the `SetExpressCheckout` response as a name-value pair where noted, and redirect the customer's browser to the following URL:

```
https://www.paypal.com/cgi-bin/webscr?cmd=_express-checkout&token=value_from_SetExpressCheckoutResponse
```

NOTE: Express Checkout has a variation on this redirect URL (called “user action”) that allows the application to bypass the second request-response pair (`GetExpressCheckoutDetails` and `GetExpressCheckoutDetailsResponse`) and change the text of the final button displayed on PayPal. For more information on this variation, see *PayPal Website Payments Pro Integration Guide*.

Recommendation for Browser Redirection

To redirect the customer's browser to the PayPal URL, PayPal recommends the HTTPS response 302 “Object Moved”, with the PayPal URL as the value of the `Location` header in the HTTPS response. Ensure that the application uses an SSL-enabled server to prevent browser warnings about a mix of secure and nonsecure graphics.

Order Review Page Setup

PayPal recommends that order review pages be set up as follows:

1. Shipping Information Section:

- Display the shipping address supplied by PayPal.
- On first use of the `SetExpressCheckout` API call, if the customer selected a shipping address stored in the PayPal account, redirect the customer's browser back to PayPal to edit the shipping address. To redirect the browser a second time, use the `SetExpressCheckout` API again, and include the `Token` that was received in the first `SetExpressCheckout` response. (On the second `SetExpressCheckout` API call, include `ReturnURL`, `CancelURL`, and other required elements only if their values are different from the values included in the first `SetExpressCheckout` API call. These values most likely will be different on the second request.)

2. Billing Information Section:

- Display the customer's PayPal email address provided in Express Checkout.

3. Order Total:

- The application must display the same exact `OrderTotal` value that was sent to PayPal in the `DoExpressCheckoutPayment` request.

Authorization & Capture

PayPal assumes that at the end of the checkout process, the merchant makes a final sale and payment transaction through PayPal. If, at the point of sale, the merchant does not know the complete cost of the order—for example, if the shipping, handling, and tax are not precisely known or there is an upsell—a transaction can be authorized that can be captured later, with Authorization & Capture.

PayPal uses Authorization & Capture in both Express Checkout and Direct Payment.

For information on Authorization & Capture, see [“Authorization & Capture APIs” on page 87](#).

Review Questions

Answers to review questions are in [Appendix A, “Answers to Review Questions.”](#)

1. On the Order Review page, from where should the application get the value of the total order?
2. In the `SetExpressCheckout` request, what is the maximum allowed value for `AMT`?
3. How much time elapses before a `TOKEN` expires?
4. Where should the PayPal checkout button appear?
5. In the `DoExpressCheckoutPayment` request, when is a value required for the parameter `TAXAMT`?

7

Direct Payment API

In this chapter, you will learn:

- How Direct Payment works
- How to use the Direct Payment API

How Direct Payment Works

The Direct Payment API allows a merchant to accept credit-card transactions directly on the merchant's website. Even though the website uses PayPal to process the credit-card transaction, this process is invisible to customers. This means customers are not taken away from the website; the website provides a single, unified look and feel.

IMPORTANT: Payments made through the Direct Payment API are not covered by the PayPal Seller Protection Policy.

The Direct Payments API is part of the Website Payments Pro solution.

The PayPal Direct Payment API calls work as follows:

1. On the website, the customer chooses to pay with a credit card and enters the credit-card number and other details.
2. The customer reviews the order.
3. When the customer clicks **Pay** to place the order, the application sends a `DoDirectPayment` request to the PayPal server, and the payment transaction is initiated.

The `DoDirectPayment` request includes required information that was collected from the customer, such as the amount of the transaction and the customer's credit-card number and expiration date, as well as the browser IP address and an element that specifies whether this transaction is a final sale (complete transaction amount including shipping, handling, and tax) or an authorization for a final amount that must be captured later with Authorization & Capture. The `DoDirectPayment` response includes a transaction identification number and other information.

NOTE: The customer does not see this step; PayPal is completely invisible to customers before, during, and after the purchase. PayPal does not send an email receipt to the customer, nor will the customer's credit-card statement indicate that PayPal processed the payment.

4. The application transfers the customer to the order-confirmation page.

Direct Payment API Reference Information

The following sections contain reference information about the parameters and fields used in the various requests and responses involved in PayPal Direct Payment.

Further reference information is available in *PayPal Name-Value Pair API Developer Guide and Reference*.

DoDirectPayment Request

Use a `DoDirectPayment` request to charge a credit card or to authorize a credit card for later capture.

TABLE 7.1 DoDirectPayment Request Parameters

Parameter	Description	Required?
METHOD	Name of the API: <code>DoDirectPayment</code>	Yes
PAYMENTACTION	How the merchant wants to obtain payment: <ul style="list-style-type: none"> • <code>Authorization</code> indicates this payment is a basic authorization subject to settlement with PayPal Authorization & Capture. • <code>Sale</code> indicates this is a final sale for which the merchant is requesting payment. Character length and limit: Up to 13 single-byte alphabetic characters	Yes
IPADDRESS	IP address of the payer's browser. PayPal records this IP address as a means of detecting possible fraud. Character length and limitations: 15 single-byte characters, including periods (for example, 255.255.255.25). Allowable values: Any valid Internet Protocol address.	Yes
AMT	Total of the order, including shipping, handling, and tax. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).	Yes
CREDITCARDTYPE	Type of credit card. Character length and limitations: Up to 10 single-byte alphabetic characters. Allowable values: <ul style="list-style-type: none"> • <code>Visa</code> • <code>MasterCard</code> • <code>Discover</code> • <code>Amex</code> 	Yes

TABLE 7.1 DoDirectPayment Request Parameters (Continued)

Parameter	Description	Required?
ACCT	Credit-card number. Character length and limitations: Numeric characters only. No spaces or punctuation. Must conform with the length required by each credit-card type.	Yes
EXPDATE	Credit-card expiration date. Format: MMYYYY Character length and limitations: 6 single-byte numeric characters, including leading 0.	Yes
FIRSTNAME	Payer's first name. Character length and limitations: 25 single-byte characters	Yes
LASTNAME	Payer's last name. Character length and limitations: 25 single-byte characters	Yes
STREET	First street address. Character length and limitations: 100 single-byte characters	No
CITY	City. Character length and limitations: 40 single-byte characters	No
STATE	State or province. Character length and limitations: 40 single-byte characters For state or province abbreviations, see <i>PayPal Name-Value Pair API Developer Guide and Reference</i> .	No
COUNTRYCODE	Country code. Character length and limitations: Two single-byte characters. For a list of country codes, see <i>PayPal Name-Value Pair API Developer Guide and Reference</i> .	No
ZIP	U.S. ZIP code or other country-specific postal code. Character length and limitations: 20 single-byte characters	No
NOTIFYURL	The URL for receiving Instant Payment Notification (IPN) about this transaction. If a URL is not specified in the request, the notification URL from the Merchant Profile is used, if one exists. Character length and limitations: 2,048 single-byte alphanumeric characters.	No

TABLE 7.1 DoDirectPayment Request Parameters (Continued)

Parameter	Description	Required?
CURRENCYCODE	A three-character currency code. Default: USD. This parameter accepts only the following currencies: <ul style="list-style-type: none"> • AUD — Australian Dollar • CAD — Canadian Dollar • EUR — Euro • GBP — Pound Sterling • JPY — Japanese Yen • USD — US Dollar 	No
ITEMAMT	Sum of the cost of all items in this order. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,). ITEMAMT is required if L_AMT <i>n</i> is specified.	No
SHIPPINGAMT	Total shipping costs for this order. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,). If a value for SHIPPINGAMT is specified, there also must be a value for ITEMAMT.	No
HANDLINGAMT	Total handling costs for this order. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,). If a value for HANDLINGAMT is specified, there also must be a value for ITEMAMT.	No
TAXAMT	Sum of the tax for all items in this order. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,). TAXAMT is required if L_TAXAMT <i>n</i> is specified.	No
DESC	Description of items the customer is purchasing. Character length and limitations: 127 single-byte alphanumeric characters	No
CUSTOM	A free-form field for the developer's own use. Character length and limitations: 256 single-byte alphanumeric characters	No

TABLE 7.1 DoDirectPayment Request Parameters (Continued)

Parameter	Description	Required?
INVNUM	The merchant's own invoice or tracking number. Character length and limitations: 127 single-byte alphanumeric characters	No
BUTTONSOURCE	An identification code for use by third-party applications to identify transactions. Character length and limitations: 32 single-byte alphanumeric characters	No
NOTIFYURL	The URL for receiving Instant Payment Notification (IPN) about this transaction. If this URL is not specified in the request, the notification URL from the Merchant Profile is used, if one exists. Character length and limitations: 2,048 single-byte alphanumeric characters	No
L_NAME <i>n</i>	Item name. Character length and limitations: 127 single-byte characters These parameters should be ordered sequentially beginning with 0 (for example, L_NAME0, L_NAME1, and so on).	No
L_NUMBER <i>n</i>	Item number. Character length and limitations: 127 single-byte characters These parameters should be ordered sequentially beginning with 0 (for example, L_NUMBER0, L_NUMBER1, and so on).	No
L_QTY <i>n</i>	Item quantity. Character length and limitations: Any positive integer These parameters should be ordered sequentially beginning with 0 (for example, L_QTY0, L_QTY1, and so on).	No
L_TAXAMT <i>n</i>	Item sales tax. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,). These parameters should be ordered sequentially beginning with 0 (for example, L_TAXAMT0, L_TAXAMT1, and so on).	No
L_AMT <i>n</i>	Cost of the item. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,). These parameters should be ordered sequentially beginning with 0 (for example, L_AMT0, L_AMT1, and so on). If a value for L_AMT <i>n</i> is specified, there must be a value for ITEMAMT.	No

TABLE 7.1 DoDirectPayment Request Parameters (Continued)

Parameter	Description	Required?
CVV2	Card Verification Value, version 2. The Merchant Account settings determine whether this field is required. Contact a PayPal Account Manager for more information. Character length for Visa, MasterCard, and Discover: Three digits. Character length for American Express: Four digits. IMPORTANT: To comply with credit-card-processing regulations, once a transaction has been completed, the application must not store the value of CVV2.	See description
EMAIL	Email address of payer. Character length and limit: 127 single-byte characters	No
STREET2	Second street address. Character length and limit: 127 single-byte characters	No
PHONENUM	Phone number Character length and limit: 20 single-byte characters	No
ShippingAddress	An optional shipping address, as described in “ ShippingAddress Parameter ” on page 153. ShippingAddress is optional, but if it is included, certain fields are required.	No

DoDirectPayment Response

A DoDirectPayment response comes from the PayPal server after a request to charge a credit card or authorize a credit card for later capture.

TABLE 7.2 DoDirectPayment Response Fields

Field	Description	Possible Values
AMT	The amount of the payment as specified in the DoDirectPayment request.	See description.
AVSCODE	Address Verification System response code. Character limit: One single-byte alphanumeric character.	See “ AVS Response Codes ” on page 155.
CVV2MATCH	Result of the CVV2 check by PayPal.	See “ CVV2 Response Codes ” on page 156.
TRANSACTIONID	Unique transaction ID of the payment. NOTE: If the PAYMENTACTION of the request was Authorization, the value of TRANSACTIONID is the AuthorizationID for use with the Authorization & Capture APIs. Character length and limitation: 19 single-byte characters.	See description.

Authorization & Capture

PayPal assumes that at the end of the checkout process, the merchant makes a final sale and payment transaction through PayPal. If, at the point of sale, the merchant does not know the complete cost of the order—for example, if the shipping, handling, and tax are not precisely known or there is an upsell—a transaction can be authorized that can be captured later, with Authorization & Capture.

PayPal uses Authorization & Capture in both Direct Payment and Express Checkout.

For more information about Authorization & Capture, see [“Authorization & Capture APIs”](#) on [page 87](#).

Review Questions

Answers to review questions are in [Appendix A, “Answers to Review Questions.”](#)

1. True or false: If the merchant’s application uses Direct Payment, the name “PayPal” does not appear on the customer’s credit-card statement.
2. How does PayPal determine if the CVV2 parameter is required in the `DoDirectPayment` request?

8

Transactions

In this chapter, you will learn:

- How to use the Authorize & Capture APIs to authorize payments without actually receiving them, and how to get authorized payments
- How to refund a customer's payment
- How to search for transactions and find details of a specific transaction
- How to use PayPal's automated payment-notification capabilities

Authorization & Capture APIs

PayPal uses Authorization & Capture in both Express Checkout and Direct Payment.

Authorization & Capture APIs provide merchants with increased flexibility in obtaining payments from their customers. Authorization & Capture separates the authorization of payment from the capture of the authorized payment.

Authorization & Capture is for merchants who have a delayed order-fulfillment process. It enables merchants to modify the original authorization amount, due to order changes occurring after the initial order is placed (such as taxes, shipping, or item availability).

Authorization & Capture allows merchants to authorize, capture, reauthorize, and void funds.

Authorization Process

1. Authorization & Capture starts when the customer authorizes a payment amount during checkout (for example, by using the PayPal Express Checkout API with the `PAYMENTACTION` element set to `Authorization`).
2. After the customer completes checkout, use the payment's transaction ID with Authorization & Capture APIs to:
 - Capture a partial amount or the full authorization amount.
 - Capture or reauthorize a higher amount, up to 115% of the originally authorized amount (not to exceed an increase of \$75 USD).
 - Void a previous authorization.

Honor Period and Authorization Period

When the customer approves an authorization, the customer's balance can be placed on hold for a 29-day period to ensure the availability of the authorization amount for capture.

The merchant can reauthorize a transaction only once, up to 115% of the originally authorized amount (not to exceed an increase of \$75 USD). After a successful reauthorization, PayPal honors 100% of the authorized funds for the first 3 days of the 29-day period. A day is defined as the start of the calendar day on which the authorization or reauthorization was made (from 12 AM PST to 11:59 PM PST).

A merchant can settle without a reauthorization from day 4 to day 29 of the authorization period, but PayPal cannot ensure that 100% of the funds will be available after the 3-day honor period. PayPal will not allow the merchant to capture funds if the customer's account is restricted or locked, a fraudulent case occurs, or the merchant's account has a high restriction level. PayPal makes its best effort to capture funds outside the honor period; however, there is a possibility that funds will not be available at that time.

Buyer and seller accounts cannot be closed if there is a pending unsettled authorization.

Authorization & Capture API Reference Information

There are three APIs related to Authorization & Capture:

- DoCapture
- DoVoid
- DoReauthorization

The following sections display reference information about the parameters and fields used in the various requests and responses involved in Authorization & Capture.

DoCapture Request

Use a DoCapture request to capture a complete or partial authorized amount.

TABLE 8.1 DoCapture Request Parameters

Parameter	Description	Required?
METHOD	Name of API: DoCapture	Yes
AUTHORIZATIONID	The authorization identification number of the payment to capture. This is the transaction ID returned from DoExpressCheckoutPayment or DoDirectPayment. Character length and limits: 19 single-byte characters maximum.	Yes
AMT	Amount to capture. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).	Yes

TABLE 8.1 DoCapture Request Parameters (Continued)

Parameter	Description	Required?
CURRENCYCODE	A three-character currency code for one of the PayPal-supported transactional currencies. Default value: USD	No
COMPLETETYPE	The value <code>Complete</code> indicates this is the last capture to make. The value <code>NotComplete</code> indicates there will be additional captures. NOTE: If <code>Complete</code> , any remaining amount of the original authorized transaction is automatically voided, and all remaining open authorizations are voided. Character length and limits: 12 single-byte alphanumeric characters.	Yes
INVNUM	The invoice number or other identification number that is displayed to the merchant and customer in the customer's transaction history. NOTE: This value in <code>DoCaptureRequest</code> will overwrite a value previously set on <code>DoAuthorizationRequest</code> . NOTE: The value is recorded only if the authorization being captured is an order authorization, not a basic authorization. Character length and limits: 127 single-byte alphanumeric characters.	No
NOTE	An informational note about this settlement that is displayed to the customer in email and in the customer's transactional history. Character length and limits: 255 single-byte characters.	No

DoCapture Response

A `DoCapture` response contains the results of a capture of authorized funds.

TABLE 8.2 DoCapture Response Fields

Field	Description
AUTHORIZATIONID	The authorization identification number specified in the request. Character length and limits: 19 single-byte characters maximum.
TRANSACTIONID	Unique transaction ID of the payment. Character length and limitations: 17 single-byte characteristics

TABLE 8.2 DoCapture Response Fields (Continued)

Field	Description
PARENTTRANSACTIONID	<p>Parent or related transaction identification number. This field is populated for the following transaction types:</p> <ul style="list-style-type: none"> • Reversal — Capture of an authorized transaction. • Reversal — Reauthorization of a transaction. • Capture of an order — The value of PARENTTRANSACTIONID is the original OrderID. • Authorization of an order — The value of PARENTTRANSACTIONID is the original OrderID. • Capture of an order authorization. • Void of an order — The value of PARENTTRANSACTIONID is the original OrderID. <p>Character length and limits: 16 digits in xxxx-xxxx-xxxx-xxxx format</p>
RECEIPTID	<p>Receipt identification number.</p> <p>Character length and limits: 16 digits in xxxx-xxxx-xxxx-xxxx format</p>
TRANSACTIONTYPE	<p>The type of transaction:</p> <ul style="list-style-type: none"> • cart • express-checkout <p>Character length and limits: 15 single-byte characters</p>
PAYMENTTYPE	<p>Indicates whether the payment is instant or delayed.</p> <p>Character length and limits: 7 single-byte characters</p>
ORDERTIME	<p>Time/date stamp of payment.</p> <p>For example: 2006-08-15T17:23:15Z</p>
AMT	<p>The final amount charged, including any shipping and taxes from the Merchant Profile.</p>
FEEAMT	<p>PayPal fee amount charged for the transaction.</p>
SETTLEAMT	<p>Amount deposited in the merchant's PayPal account if there is a currency conversion.</p>
TAXAMT	<p>Tax charged on the transaction, if any.</p>
EXCHANGERATE	<p>Exchange rate if a currency conversion occurred. Relevant only if the merchant is billing a currency other than the customer's primary currency. If this is the case, the conversion occurs in the customer's account.</p> <p>Character length and limitations: a decimal multiplier</p>

TABLE 8.2 DoCapture Response Fields (Continued)

Field	Description
PAYMENTSTATUS	<p>The status of the payment:</p> <ul style="list-style-type: none"> • None — No status. • Canceled-Reversal — A reversal was canceled. For example, the merchant won a dispute with the customer, and the funds for the transaction that was reversed were returned. • Completed — The payment was completed, and the funds were added successfully to the merchant’s account balance. • Denied — The merchant denied the payment. This happens only if the payment was previously pending because of possible reasons described in the PENDINGREASON element. • Expired — The authorization period for this payment was reached. • Failed — The payment failed. This happens only if the payment was made from the customer’s bank account. • Pending — The payment is pending. For more information, see the PENDINGREASON field. • Refunded — The merchant refunded the payment. • Reversed — A payment was reversed due to a chargeback or other type of reversal. The funds were removed from the merchant’s account balance and returned to the customer. The reason for the reversal is specified in the REASONCODE element. • Processed — A payment was accepted. • Voided — An authorization for this transaction was voided.

DoVoid Request

Use a DoVoid request to request a void for an authorization.

TABLE 8.3 DoVoid Request Parameters

Parameter	Description	Required?
METHOD	Name of API: DoVoid	Yes
AUTHORIZATIONID	<p>The value of the original authorization identification number returned by PayPal.</p> <p>IMPORTANT: If the merchant is voiding a transaction that was reauthorized, use the ID from the original authorization, not the reauthorization.</p> <p>Character length and limits: 19 single-byte characters</p>	Yes
NOTE	<p>An informational note about this void that is displayed to the customer in email and in the transaction history.</p> <p>Character length and limits: 255 single-byte characters</p>	No

DoVoid Response

A `DoVoid` response contains the results of an authorization void.

TABLE 8.4 DoVoid Response Fields

Field	Description
AUTHORIZATIONID	The authorization identification number specified in the request. Character length and limits: 19 single-byte characters

DoReauthorization Request

Use a `DoReauthorization` request to request a reauthorization for a given amount of money.

TABLE 8.5 DoReauthorization Request Parameters

Parameter	Description	Required?
METHOD	Name of API: <code>DoReauthorization</code>	Yes
AUTHORIZATIONID	The value of a previously authorized transaction identification number returned by PayPal. Character length and limits: 19 single-byte characters maximum	Yes
AMT	Amount to authorize. Limitations: Must not exceed \$10,000 USD in any currency. No currency symbol. Must have two decimal places, decimal separator must be a period (.), and the optional thousands separator must be a comma (,).	Yes
CURRENCYCODE	A three-character currency code for one of the PayPal-supported transactional currencies. Default value: USD	No

DoReauthorization Response

A `DoReauthorization` response contains the results of the reauthorization.

TABLE 8.6 DoReauthorization Response Fields

Field	Description
AUTHORIZATIONID	A new authorization identification number. Character length and limits: 19 single-byte characters

Authorization & Capture Best Practices

The following sections describe the best practices to follow in using Authorization & Capture, to ensure the best buying experience for customers and get the most benefit from Authorization & Capture.

Capturing Funds on Basic Authorizations

PayPal recommends that a merchant capture funds within the honor period of three days, because PayPal will honor the funds for a three-day period after the basic authorization. If the merchant tries to capture funds after the three-day period and the authorization fails, the request to capture funds may be denied.

After day 4 of the authorization period, a merchant can initiate a reauthorization, which starts a new three-day honor period; however, the reauthorization does not extend the original authorization period past 29 days.

The merchant should capture funds within 24 hours after shipping the customer's order.

Customer Approval for Basic Authorizations

A customer-initiated authorization allows the merchant to capture funds from the customer's account of up to 115% of the originally authorized amount (not to exceed an increase of \$75 USD) and up to \$10,000 USD (the limit for a single purchase through PayPal).

IMPORTANT: If the merchant wants to update any details of the purchase that change the original authorization amount, PayPal requires that the merchant obtain consent from the customer at the time of purchase or at the time of capture.

Voiding Basic Authorizations

The merchant should void an authorization if the authorization or reauthorization will not be used. Voiding the authorization unlocks the temporary hold placed on the customer's funding sources.

For More Information

For more information on all capabilities of Authorization & Capture, including order authorization, see the PayPal documentation available through the Integration Center.

Refunds

A merchant can refund the full amount or a partial amount of a transaction with the `RefundTransaction` API.

RefundTransaction Request

Use a `RefundTransaction` request to initiate a full or partial refund of a transaction.

TABLE 8.7 *RefundTransaction Request Parameters*

Parameter	Description	Required?
METHOD	Name of API call: <code>RefundTransaction</code>	Yes
TRANSACTIONID	Unique identifier of a transaction. Character length and limitations: 17 single-byte alphanumeric characters	Yes
REFUNDTYPE	Type of refund to make: <ul style="list-style-type: none"> • Full • Partial • Other 	Yes
AMT	Refund amount. AMT is required if REFUNDTYPE is <code>Partial</code> . NOTE: If REFUNDTYPE is <code>Full</code> , do not set AMT.	No
NOTE	Custom memo about the refund. Character length and limitations: 255 single-byte alphanumeric characters	No

RefundTransaction Response

A `RefundTransaction` response contains the results of the refund.

TABLE 8.8 *RefundTransaction Response Fields*

Field	Description
REFUNDTRANSACTIONID	Unique transaction ID of the refund. Character length and limitations: 17 single-byte characters
NETREFUNDAMT	Amount subtracted from PayPal balance of original recipient of payment to make this refund.
FEEREFUNDAMT	Transaction fee refunded to original recipient of payment.
GROSSREFUNDAMT	Amount of money refunded to original payer.

Transaction Searches

To find all transactions that occurred on a particular date, use the `TransactionSearch` API. The date must be in UTC/GMT format.

With `TransactionSearch`, always set the `StartDate` field. Also note the following:

- Setting `TransactionID` overrides all other fields (including `StartDate`).
- The effect of setting other elements is additive or can alter the search criteria.

`TransactionSearch` returns up to 100 matches. Partial matches are displayed. For example, setting the `FirstName` parameter of the `TransactionSearch` request to “Jess” returns results including “Jessica” and “Jesse.”

The most important element returned in the `TransactionSearch` response is `TransactionID`, which can be passed to `GetTransactionDetails` to retrieve all available information about a specific transaction. For more information on the `GetTransactionDetails` API, see [“Retrieving Transaction Details” on page 98](#).

TransactionSearch Request

Use a `TransactionSearch` request to search for transactions that occurred on a given date.

TABLE 8.9 *TransactionSearch Request Parameters*

Parameter	Description	Required?
METHOD	Name of API call: <code>TransactionSearch</code>	Yes
STARTDATE	The earliest transaction date at which to start the search. No wildcards are allowed. The value must be in UTC/GMT format.	Yes
ENDDATE	The latest transaction date to be included in the search.	No
EMAIL	Search by the customer’s email address. Character length and limitations: 127 single-byte alphanumeric characters.	No
RECEIVER	Search by the receiver’s email address. If the merchant account has only one email, this is the primary email. This also can be a nonprimary email.	No
RECEIPTID	Search by the PayPal Account Optional receipt ID.	No
TRANSACTIONID	Search by the Transaction ID. The returned results are from the merchant’s transaction records. Character length and limitations: 19 single-byte characters maximum.	No

TABLE 8.9 TransactionSearch Request Parameters (Continued)

Parameter	Description	Required?
INVNUM	Search by the invoice identification key, as set for the original transaction. This field searches the records for items sold by the merchant, not for items purchased. No wildcards are allowed. Character length and limitations: 127 single-byte characters maximum.	No
ACCT	Search by credit-card number, as set for the original transaction. This field searches the records for items sold by the merchant, not for items purchased. No wildcards are allowed. Character length and limitations: Must be at least 11 and no more than 25 single-byte numeric characters maximum. Special punctuation, such as dashes or spaces, is ignored.	No
SALUTATION	Customer's salutation. Character length and limitations: 20 single-byte characters	No
FIRSTNAME	Customer's first name. Character length and limitations: 25 single-byte characters	No
MIDDLENAME	Customer's middle name. Character length and limitations: 25 single-byte characters	No
LASTNAME	Customer's last name. Character length and limitations: 2025 single-byte characters	No
SUFFIX	Customer's suffix. Character length and limitations: 12 single-byte characters	No
AUCTIONITEMNUMBER	Search by auction item number of the purchased goods.	No

TABLE 8.9 TransactionSearch Request Parameters (Continued)

Parameter	Description	Required?
TRANSACTIONCLASS	<p>Search by classification of transaction.</p> <p>Some possible classes of transactions are not searchable with this field (for example, bank-transfer withdrawals).</p> <p>The following classes of transaction can be searched for:</p> <ul style="list-style-type: none"> • All — All transaction classifications • Sent — Only payments sent • Received — Only payments received • MassPay — Only mass payments • MoneyRequest — Only money requests • FundsAdded — Only funds added to balance • FundsWithdrawn — Only funds withdrawn from balance • Referral — Only transactions involving referrals • Fee — Only transactions involving fees • Subscription — Only transactions involving subscriptions • Dividend — Only transactions involving dividends • Billpay — Only transactions involving BillPay Transactions • Refund — Only transactions involving refunds • CurrencyConversions — Only transactions involving currency conversions • BalanceTransfer — Only transactions involving balance transfers • Reversal — Only transactions involving BillPay Reversals • Shipping — Only transactions involving UPS shipping fees • BalanceAffecting — Only transactions that affect the account balance • ECheck — Only transactions involving eCheck 	No
AMT	Search by transaction amount.	No
STATUS	<p>Search by transaction status:</p> <ul style="list-style-type: none"> • Pending — The payment is pending. The specific reason the payment is pending is returned by the <code>GetTransactionDetails</code> API. • Processing — The payment is being processed. • Success — The payment was completed, and the funds were added successfully to the merchant's account balance. • Denied — The merchant denied the payment. This happens only if the payment was previously pending. • Reversed — A payment was reversed due to a chargeback or other type of reversal. The funds were removed from the merchant's account balance and returned to the customer. 	No

TransactionSearch Response

A `TransactionSearch` response contains the results of the transaction search.

NOTE: Each of these parameters should be numbered sequentially beginning with 0 (for example, `L_TIMESTAMP0`, `L_TIMESTAMP1`, `L_TIMESTAMP2`, and so on).

TABLE 8.10 *TransactionSearch Response Fields*

Field	Description
<code>L_TIMESTAMPn</code>	Date and time (in UTC/GMT format) the transaction occurred.
<code>L_TIMEZONEn</code>	Time zone of the transaction.
<code>L_TYPEn</code>	Type of the transaction.
<code>L_EMAILn</code>	Email address of the payer or the payment recipient (the “payee”). If the payment amount is positive, this field is the recipient of the funds. If the payment is negative, this field is the paying customer.
<code>L_NAMEn</code>	Display name of the payer.
<code>L_TRANSACTIONIDn</code>	Seller’s transaction ID.
<code>L_STATUSn</code>	Status of the transaction.
<code>L_AMTn</code>	Total gross amount charged, including any profile shipping cost and taxes.
<code>L_FREEAMTn</code>	Fee that PayPal charged for the transaction.
<code>L_NETAMTn</code>	Net amount of the transaction.

Retrieving Transaction Details

If the merchant has the Transaction ID of a transaction, the merchant can retrieve all of the details about that transaction from the PayPal server.

NOTE: The details for some kinds of transactions cannot be retrieved with `GetTransactionDetails` (for example, bank transfer withdrawals).

GetTransactionDetails Request

Use a `GetTransactionDetails` request to search for a specific transaction.

TABLE 8.11 *GetTransactionDetails Request Parameters*

Parameter	Description	Required?
METHOD	Name of the method: <code>GetTransactionDetails</code>	Yes
TRANSACTIONID	Unique identifier of a transaction. Character length and limitations: 17 single-byte alphanumeric characters.	Yes

GetTransactionDetails Response

A `GetTransactionDetails` response contains all the details and information on the specified transaction.

The complete list of parameters returned by the `GetTransactionDetails` response is documented in *PayPal Name-Value Pair API Developer Guide and Reference*.

Payment Notification Integration

Website Payments Pro offers multiple payment notification methods, including:

- Email
- Reporting Tools
- Instant Payment Notification (IPN)

Email

Merchants automatically receive an email notification in the following cases:

- Successful payment
- Pending payment
- Canceled payment

To turn off payment notifications through email, follow these steps:

1. In the **My Account** tab, click the **Profile** subtab.
2. In the **Account Information** column, click the **Notifications** link.
3. Find the **Payment Notifications** heading, and clear the **I receive PayPal Website Payments and Instant Purchase** checkbox.
4. Click **Save**.

Reporting

Paypal Reporting Tools provide the information necessary to effectively measure and manage a business. With PayPal Reporting Tools, merchants can:

- Analyze revenue sources to better understand customers' buying behaviors.
- Automate time-consuming bookkeeping tasks.
- Accurately settle and reconcile transactions.

The following reports are available:

- **Monthly Account Statements** — Every month, view a summary of all credits and debits that affect the account balance.
- **Merchant Sales Reports** — Every week, receive a valuable analysis of revenue by sales channel and currency.
- **History Log** — View an online record of received and sent payments.
- **Downloadable Logs** — Keep track of transaction history by downloading it into various file formats (suitable for financial settlements).

For more information about PayPal reports, see the PayPal Reporting Tools website (<http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/reports-intro-outside>).

Instant Payment Notification (IPN)

IPN provides immediate notification and confirmation of PayPal payments received. IPN consists of three parts:

1. A customer issues payment from one of a number of processes (Website Payments Standard FORMS, the Express Checkout APIs, MassPay, or a refund).
2. PayPal posts FORM variables to a URL specified by the merchant (either globally in the Profile or on a per-transaction basis with the NOTIFYURL variable) that runs a program to process the variables. The customer's payment information (such as customer name and payment amount) is included in the notification.
3. The server validates the notification to ensure it is legitimate.

Because credit-card and bank information are not transmitted in IPN, PayPal does not require SSL to encrypt IPN transmissions.

Activating IPN

There are two ways to activate IPN:

- Include the NOTIFYURL variable in the DoDirectPayment or DoExpressCheckoutPayment API call. Doing this activates IPN on a per-transaction basis.
- In the merchant's PayPal profile, under **Selling Preferences**, click **Instant Payment Notification Preferences**, click **Edit**, click the checkbox and enter the URL of the program

that will process the IPN posts, and click **Save**. Doing this activates IPN for all transactions.

Setting Up an IPN-Processing Program

The data sent by IPN is in the form of name-value pairs. At a minimum, a program must process these pairs; other processing may be necessary based on the merchant's order management needs, database, and other factors outside the scope of this guide.

Code samples for several environments are available at <http://www.paypal.com/ipn>.

IPN Notification Validation

After the server receives an IPN, the merchant must confirm it was received. This is known as *notification validation*, which is a means for PayPal to help prevent spoofing or “man-in-the-middle” attacks.

A merchant can validate the notification in one of two ways:

- Send a shared secret that is known only to the merchant. PayPal recommends this method because it ensures the validity of the data and decreases network traffic to and from the merchant's website. Shared secret validation is appropriate if:
 - The merchant is not using a shared website hosting service.
 - The merchant has enabled SSL on the web server.
 - The merchant is using PayPal Encrypted Website Payments (EWP).
 - The merchant uses the NOTIFYURL variable on each individual payment transaction.
- Send a POST back to PayPal after receiving the IPN and verifying the correctness of the data. Postback is appropriate if:
 - The merchant relies on a shared hosting service.
 - The merchant does not have SSL enabled on the web server.

Both concepts rely on a *notification URL*, which is the URL to which PayPal posts IPN data. The notification URL can be set either with each transaction (if the merchant wants to receive notifications for different transactions at different URLs) or globally in the Profile.

Set the notification URL on a per-transaction basis with the NOTIFYURL variable, which must be URL-encoded. If the merchant sets the notification URL in the Profile, specifying the NOTIFYURL variable overrides the value in Profile.

NOTE: If the merchant does not use EWP or shared secret validation, he must check the price, transaction ID, PayPal receiver email address, and other data sent by IPN to ensure they are correct.

Shared Secret Validation. The recommended method for notification validation is to use a shared secret on individual payment transactions. Add a shared secret variable and value to the NOTIFYURL variable to which the IPN data is posted after a payment is made. The shared secret consists of the following:

`NOTIFYURL=IPNnotificationURL?shared_secret_variable_name=shared_secret_value`

where:

- `IPNnotificationURL` is the notification URL.
- `shared_secret_variable_name` is any variable name.
- `shared_secret_value` is the shared secret itself.

The merchant can also specify a shared secret in his Profile, which is used for all transactions. Specifying a shared secret in the `NOTIFYURL` variable explicitly overrides the value in the Profile.

NOTE: The value of the shared secret is not encrypted; it is in clear text for easier processing; therefore, the shared secret value is recorded in the merchant's web server's access logs. Always practice proper security for server access logs.

HTTPS Postback to PayPal. The second method for validating receipt of an IPN is to post the exact variables and values received in the IPN back to PayPal.

The guidelines for constructing the IPN HTTPS `POST` to PayPal for notification validation are as follows:

1. The `POST` must be sent to <https://www.paypal.com/cgi-bin/webscr>.
2. Include the variable `cmd` with the value `validate`.
3. Post all the form variables exactly as they were received.

PayPal responds to the postback with a single word in the body of the response: `VERIFIED` or `INVALID`.

After receiving a `VERIFIED` response, perform the following checks before updating a database. Move on to the next check in the sequence only if the previous one passes.

1. Check that `payment_status` is `COMPLETED`.
2. Check `txn_id` against the previous PayPal transaction, to ensure it is not a duplicate.
3. Make sure `receiver_email` is an email address registered in the merchant's PayPal account.
4. Check that the price (`mc_gross`) and currency (`mc_currency`) are correct for the item, `item_name`, or `item_number`.
5. Check that the shared secret is correct.

In the case of an `INVALID` response, further investigation is necessary; in some cases, the response is caused by an IPN error, possibly from a change in the IPN format. To determine if it is an IPN error, first examine the IPN code. For further assistance, go to <http://www.paypal.com/wf>, click **Seller Tools**, and click **Instant Payment Notification**.

Dispute Notification

Customers can register claims about payments; these claims are called *cases*. PayPal notifies merchants about new cases with email and with IPN.

There are two kinds of cases:

- A *complaint* occurs when a customer uses the PayPal Resolution Center to register a complaint about a payment to a merchant.
- A *chargeback* occurs when a customer files a complaint with a credit-card company, and the credit-card company issues a chargeback. The credit-card company notifies PayPal about the reason for the chargeback; after investigating the case, PayPal notifies the merchant of any action required.

The IPN messages for chargebacks resulting from a complaint are asynchronous; that is, the IPN message for the chargeback can be sent to the merchant before the IPN message related to the complaint. Compare the IPN variable `parent_txn_id` of all IPN messages to match the chargeback with the complaint.

IPN variables for cases include the type of case, the reason, and other information about the case. For a complete list of IPN variables, see *PayPal Order Management Integration Guide*.

Review Questions

Answers to review questions are in [Appendix A, “Answers to Review Questions.”](#)

1. What percentage of the originally authorized amount can be authorized by using the payment’s transaction ID?
2. True or false: Initiating a reauthorization after day 4 of the authorization period extends the entire authorization period by three days (from 29 days to 32 days).
3. In a `RefundTransaction` request, if `REFUNDTYPE` is `Full`, what should `AMT` be set to?
4. True or false: Merchants can search for transactions that involve only mass payments.
5. Is SSL required for encrypting IPN transmissions?
6. What is the difference between a complaint and a chargeback?

9

Sandbox Testing

In this chapter, you will learn:

- How to set up test users in the Sandbox
- How to test various aspects of an integrated e-commerce application in the Sandbox
- How to migrate the application to use the live PayPal server

Overview

The PayPal Sandbox is a self-contained environment within which you can prototype and test PayPal features and APIs without using real money or impacting your production system's PayPal accounts. The PayPal Sandbox is an almost-identical copy of the live PayPal website. Its purpose is to give developers a shielded environment for testing and integration purposes, to help avoid problems that might occur while testing PayPal integration solutions on the live site. Before moving any PayPal-based application into production, test the application in the Sandbox to ensure that it functions as you intend.

At a Glance: Differences between the Sandbox and Live PayPal

Table 9.1 compares the Sandbox and Live PayPal. This is a high-level view of the differences from a developer's perspective. You also can use this table as a checklist.

TABLE 9.1 Differences between PayPal Sandbox, and Live PayPal



Item	PayPal Sandbox	Live PayPal Website and API Service
Type of PayPal Accounts	Depending on the feature you want to develop and test, you need a Personal, Business, or Premier account.	Personal, Business, or Premier account
Site logos in upper left corner	https://www.sandbox.paypal.com 	https://www.paypal.com 
NVP API Servers	https://api.sandbox.paypal.com/nvp/	For API certificate security: https://api.paypal.com/nvp/ For API signature security: https://api-3t.paypal.com/nvp/

TABLE 9.1 Differences between PayPal Sandbox, and Live PayPal (Continued)

Item	PayPal Sandbox	Live PayPal Website and API Service
SOAP API Servers	https://api.sandbox.paypal.com/2.0/	For API certificate security: https://api.paypal.com/2.0/ For API signature security: https://api-3t.paypal.com/2.0/
Business roles	You fill all roles you need to test: merchant, buyer, and seller.	Real-world people fill these roles.
Company and people's names and postal addresses	Completely fictitious. Before you begin working with the Sandbox, create the details for all the business roles you must fulfill. The Sandbox simulates verification of postal addresses and names.	Real companies' and people's names and postal addresses.
Email addresses and email inboxes	The Sandbox has a special-purpose email inbox for your testing, contained in the Sandbox itself.	Real email address and inbox for each business role
Bank account and credit card numbers	The Sandbox creates bank accounts, credit-card numbers, and CVV2 numbers you need to develop and test; all of these are fictitious and used only within the Sandbox. The Sandbox simulates the verification of these numbers. Transactions do not affect real accounts, and money is never exchanged.	Actual verification of bank account numbers, credit-card numbers, and CVV2 numbers
Social Security Number for Billing Agreements	111- <i>nn-nnnn</i>	Real Social Security Numbers
PayPal transactions	The Sandbox creates all fictitious bank accounts, credit-card numbers, and CVV2 numbers you need for development and testing. The Sandbox simulates the verification of these numbers.	Live transactions, cleared by live PayPal processes
Fraud detection	Fraud detection is not enabled for the Sandbox.	Full protection through PayPal's fraud detection

TABLE 9.1 Differences between PayPal Sandbox, and Live PayPal (Continued)

Item	PayPal Sandbox	Live PayPal Website and API Service
Digital certificates	After you request digital certificates for use with the PayPal Web Services API, the Sandbox automatically generates them. They are available for immediate downloading.	To safeguard your and your customers' security, requests for digital certificates for use with the Live PayPal Web Services API must be verified by PayPal before they are issued. You are notified in email when your request is approved.
PayPal Merchant Features supported	All features of the live PayPal website, except closing an account, auction features, monthly statements, shipping preferences, and PayPal Shops.	

Accessing the PayPal Sandbox

To access the PayPal Sandbox, sign up for an account at <https://developer.paypal.com>. After signing up, you access the Sandbox programmatically or by logging in.

Depending on the PayPal feature you want to test with an application, you need to set up different types of test accounts: PayPal Personal (or Premier) and Business accounts. See “Planning the Types of Test Accounts You Need” on page 111.

Signing Up for Sandbox Access

To sign up for Sandbox access, follow these steps:

1. Go to <https://developer.paypal.com>. The login screen is shown below:

The screenshot shows the PayPal Developer Central website. At the top left is the PayPal logo and "Developer Central". At the top right are links for "PayPal Home" and "Contact Us". The main content area is divided into two columns. The left column contains a "Member Log In" section with fields for "Email Address" and "Password", a checkbox for "Log me in automatically", a "Log In" button, and a link for "Trouble Logging In?". Below this is a "Can We Help?" section with text about the PayPal Developer Community and a "Sign Up Now" button. The right column features a large banner with the text "PayPal Sandbox Put your code to the test" and a "Sign Up Now" button. Below the banner is a section titled "Need an account? Sign up now to access PayPal's Sandbox Test Environment." with a "Sign Up Now" button and a paragraph of text. At the bottom of the page is a dark blue footer with links for "Fees", "Privacy", "Security Center", "Contact Us", and "User Agreement", along with "PayPal, an eBay Company", copyright information, and logos for "TRUSTe" and "BBB ONLINE".

2. If you already have an account, enter your Log In Email and Password and click **Log In**.

3. If you do not already have an account, click **Sign Up Now** and provide the requested information shown below:

Sign Up for Access to the Sandbox Test Environment

This account will allow you to use the PayPal Sandbox Test Environment to try out Website Payments, Instant Payment Notification, PayPal APIs, and other features.

First Name:

Last Name:

Email Address:
Do not use your PayPal account login email.

Password:
At least 8 characters long, case sensitive.

Confirm Password:

Security Question: -- select a question --

Security Answer:

Communications: Please keep me informed on PayPal's Web Services, the PayPal Sandbox, and Developer Central.

Terms of Use - The User Agreement and Privacy Policy are designed to protect and inform you of your rights within the PayPal Developer Central service.

User Agreement [\(Printer Friendly Version\)](#)

THE FOLLOWING DESCRIBES THE TERMS ON WHICH PAYPAL OFFERS YOU ACCESS TO OUR PAYPAL DEVELOPER CENTRAL SERVICES.

This User Agreement ("Agreement") is a contract between you and PayPal, Inc. and applies to your use of the PayPal Developer

Privacy Policy [\(Printer Friendly Version\)](#)

The Privacy Policy below governs your PayPal Developer Central account and any information you provide on the PayPal Developer Central site.

A. Overview

Do you agree to the User Agreement and Privacy Policy, and terms incorporated therein?

Yes No

IMPORTANT: Do not use the same login email address or password that you use for logging into the live `paypal.com` site, because later you may allow someone to work in the Sandbox on your behalf but not want to allow access to your regular PayPal account.

You can specify the same password (not email address) for all your test accounts, so you can more easily remember it.

After you sign up, PayPal sends login instructions to the email address you used to sign-up. If you have mail filtering enabled in your mail software, the email sent by PayPal might be filtered out or stored in a folder where you do not expect it to be located. For instance, with Microsoft Outlook mail software, your filtering might cause the email to be stored in "Junk" or "Spam."

4. Respond to the confirmation e-mail and log in.

Welcome to the PayPal Sandbox

When you log in to the Sandbox, the Sandbox Test Environment home page appears:

The screenshot shows the PayPal Developer Central Sandbox Test Environment home page. At the top, the PayPal logo and 'Developer Central' are displayed, along with links for Help, Profile, and Log Out. A navigation menu on the left lists 'Sandbox', 'Home', 'Test Accounts', 'Test Email', and 'API Credentials'. The main content area features a banner with the text 'PayPal Sandbox Put your code to the test'. Below the banner, a 'Can We Help?' section suggests visiting the PayPal Developer Community. The main content area lists three key actions: 'Test Accounts' (Create accounts to test your PayPal interface), 'Test Email' (Access email sent to your test accounts), and 'API Credentials' (Manage API credentials for your test accounts). The footer contains links for Fees, Privacy, Security Center, Contact Us, and User Agreement, along with copyright information and trust seals from TRUSTe and BBBONLINE.

On this page, you can perform the following actions:

- Manage test accounts from the **Test Accounts** tab. You can create and delete test accounts, and enter the Sandbox Test Site, which simulates the live `paypal.com` site. For more information, see [“Setting Up Test Accounts” on page 111](#).
- Access email sent to test accounts from the **Test Email** tab. For more information, see [“Test Email” on page 110](#).
- View API credentials for business test accounts from the **API Credentials** tab. An API signature, which is the preferred kind of credential, is created automatically when you create a Business test account. You need the information on this tab when you test APIs.
- Obtain technical information about PayPal products and APIs, using the **Help** link.
- Change the login password, using the **Profile** link.

NOTE: You cannot change the Log In Email address.

Test Email

When certain kinds of transactions occur in the live PayPal system, PayPal sends email messages to the real email addresses of the participants. From these email messages, the recipient or initiator of an event or transaction can verify that the event took place and the monetary amounts associated with the event are correct.

PayPal test email, however, is a self-contained email system in the Sandbox itself. You see email messages addressed only to the Sandbox test accounts you set up. Up to 30 of the latest email messages are listed on the **Test Email** tab. The subject lines of unread email messages are in boldface. To read the message, click a subject line.

Setting Up Test Accounts

Depending on the business application you are developing and testing, you need different types of test accounts. There are two types of test accounts: Personal (or Premier) and Business.

Planning the Types of Test Accounts You Need

You need to determine the types of test accounts you need to test the applications you are developing. In addition, you must determine the number of different accounts you need. Typically, you create at least one seller (Business) account and one buyer (Personal or Premier) account. You might need several different Personal or Business PayPal test accounts to test your application.

When you create a test account, the following information is generated for you:

- Mailing address
- Email address and password for the test PayPal account. You can specify the same password (not email address) for all your test accounts, so you can more easily remember it.
- Security questions and answers. You can use the same security questions and answers for all your test accounts, so you can more easily remember them.

IMPORTANT: Never use real email addresses or live `paypal.com` passwords for a test account. Only use fictitious information in your answers to the security questions. All this data should be fictional.

- Personal or Business account
- Your agreement to the terms of using the Sandbox

For Business accounts, the following additional information is generated for you:

- Business name and address
- Customer-service contact information
- Business-owner contact information
- Business-owner address
- Social Security Number to sign up for Website Payments Pro

Managing Test Accounts

You can view, work with, or launch the Sandbox Test Site for all your test accounts. You also can create new accounts or remove test email addresses from your view.

- To work with test accounts, log in to <https://developer.paypal.com>, and click the **Test Accounts** tab.
- To create a new account, click the **Create Account** link.
- To work with the account, select it by clicking the radio button associated with it on the left.

To simulate the live `paypal.com` site for the selected account, click **Enter Sandbox Test Site**. When you logged in to <https://developer.paypal.com>, if you set the **Log me in automatically** checkbox to allow direct access to <https://www.sandbox.paypal.com/>, you do not have to launch the Sandbox to access it.

NOTE: The **Delete** button does not delete the test account. It removes the test account from your list of accounts, but the email address for the test account is still on file for the Sandbox. You cannot re-use an email address that is still on file for the Sandbox.

Creating a Personal Account

To create a buyer with a Personal or Premier account, follow these steps:

1. After logging in, select **Test Accounts** and click the **Create Test Account** link.
2. For the **Account Type**, choose **Buyer**. Make other selections or accept the defaults. See the screenshot below.

Sandbox
Home
Test Accounts
Test Email
API Credentials

Can We Help?
Visit the [PayPal Developer Community](#) to get answers to integration questions or to file a support ticket.

PayPal Sandbox

Create a Sandbox Test Account

After creating the account, you can delete the account or you can provide additional information in the Sandbox Test Site.

Country:

Account Type: Buyer (Use to represent your customer's experience)
 Seller (Use to represent yourself as the merchant)

Login Email: @gmail.com
This email address is only used inside the Sandbox.

Password:
Your password must be at least 8 characters.

Hide Advanced Options

Add Credit Card:

Add Bank Account: Yes (Required for Confirmed account status)
 No

Confirm Email: Yes (Required for Confirmed account status)
 No

Account Balance: \$.00 USD

3. Click **Create Account**. The result is shown below.

Sandbox
Home
Test Accounts
Test Email
API Credentials

Can We Help?
Visit the [PayPal Developer Community](#) to get answers to integration questions or to file a support ticket.

PayPal Sandbox

Test Accounts

You have successfully created a test account. You can view email for this account on the Test Email tab.

Your test accounts are listed below. You must have a test business account to represent a merchant and a test personal account to represent a buyer. To simulate an action on the live site (paypal.com), select a test account and click Enter Sandbox Test Site. [Learn More](#)

Test Accounts					> Create Test Account
Login Email	Type	Country	Status	Test Mode	
buyer_1191002706_per@gmail.com	Personal	United States	Verified	N/A	View Details

NOTE: The Login Email is a pseudo-randomized address, based on the address you specified. Credit-card and bank-account numbers also are generated randomly.

Creating a Business Account

To create a seller with a Business account, follow these steps:

1. After logging in, select **Test Accounts** and click the **Create Test Account** link.
2. For the **Account Type**, choose **Seller**. Make other selections or accept the defaults. See the screenshot below.

The screenshot shows the 'Create a Sandbox Test Account' form in the PayPal Sandbox interface. On the left is a navigation menu with 'Sandbox' (Home, Test Accounts, Test Email, API Credentials) and a 'Can We Help?' section. The main form area has a 'PayPal Sandbox' header and a sub-header 'Create a Sandbox Test Account'. Below this is a note: 'After creating the account, you can delete the account or you can provide additional information in the Sandbox Test Site.' The form fields include: 'Country' (United States), 'Account Type' (Seller selected), 'Login Email' (seller@gmail.com), 'Password' (12345678), 'Add Credit Card' (Visa), 'Add Bank Account' (Yes selected), 'Confirm Email' (Yes selected), and 'Account Balance' (\$0.00 USD). At the bottom right are 'Create Account' and 'Cancel' buttons.

3. Click **Create Account**. The result is shown below.

Test Accounts



You have successfully created a test account. You can view email for this account on the Test Email tab.

Your test accounts are listed below. You must have a test business account to represent a merchant and a test personal account to represent a buyer. To simulate an action on the live site (paypal.com), select a test account and click Enter Sandbox Test Site. [Learn More](#)

Test Accounts					» Create Test Account
Login Email	Type	Country	Status	Test Mode	
<input checked="" type="radio"/> seller_1191260733_biz@gmail.com	Business	United States	Verified	Disabled	
View Details					
<input type="radio"/> buyer_1191002706_per@gmail.com	Personal	United States	Verified	N/A	
View Details					

[Enter Sandbox Test Site](#) [Delete](#)

NOTE: The Login Email is a pseudo-randomized address, based on the address you specified. Credit-card and bank-account numbers also are generated randomly.

Verified Account Status

By default, a test account has a confirmed bank account and email addresses. To create an unverified account, change the bank account to unconfirmed.

Adding a Funding Source

To test transactions, you must add a source of funds to your buyer test account. The following sections describe your choices.

1. [“Changing or Adding Additional Bank Accounts” on page 115](#). You can add bank accounts, but they will not contain funds unless you use Send Money to send the money to the bank-account holder.
2. [“Adding Credit Cards” on page 117](#). For testing, this is the most efficient way to add funds.

NOTE: No money or funds are transferred in the Sandbox; however, to protect confidentiality, do not use actual credit-card numbers or bank accounts if you allow other people to log in to your Sandbox account.

Changing or Adding Additional Bank Accounts

You add a bank account to the Sandbox test account representing a customer or buyer so you can test transactions between the buyer’s account and another account; typically, the other account is a business account that represents yourself as a merchant. Adding a bank account also changes the account status from “Unverified” to “Verified.”

The bank account is a source of funds for a user's PayPal account and, thus, for transactions between that test account and other test accounts. A test account can have multiple bank accounts, but at least one is required to verify the test account.

The Sandbox automatically generates bank-account and sort-code numbers when you add a bank account.

For Australia, Canada, Germany, or UK. Use the automatically generated bank-account information only for test US bank accounts. To add test Canadian, German, or UK bank-account information, follow the guidelines below:

- Australia:
 - BSB Number: 242-200
 - Account Number: any random number
- Canada:
 - Transit number: 00001
 - Institution number: 311
 - Bank-account number: Any 1- to 12-digit number
- Germany:
 - Routing number: 37020500
 - Bank-account number: Any 10-digit number
 - Sort code: Any 8-digit number
- UK:
 - Bank-account number: Any 8-digit number
 - Sort code: 609204 or 700709

Steps for All Countries. Follow these steps:

1. Select a test account and click **Enter Sandbox Test Site**.
2. Navigate to **My Account > Profile**.
3. Under the **Financial Information** header, click the **Bank Accounts** link.
4. In the **Bank Account** window, click **Add**.
5. In the **Add Bank Account** window:
 - Enter a fictitious bank name. Using the automatically generated bank-account number as the name of the bank makes that account number visible to you for use in testing later.
 - Except for UK or German test bank accounts, leave all other automatically generated information as is.
 - Make a note of the test bank-account number, because it will be handy to have when you do your testing.
 - Click **Add Bank Account**.

6. In the resulting success window, click the **Continue** button at the bottom. The **My Account > Overview** page opens.
7. Click the **Confirm Bank Account** link in the **Activate Account** box at the left side.
8. In the **Confirm Bank Account** window, click **Submit**.

Adding Credit Cards

A credit card is a source of funds for the buyer's PayPal account; thus, it can be used for transactions between a buyer's test account and other test accounts. A test account can have multiple credit cards. Test credit-card numbers cannot be used to pay for real-world transactions.

To create additional credit-card accounts for an already existing test account, follow these steps:

1. Select a buyer's test account, and click **Enter Sandbox Test Site**.
2. Navigate to **My Account > Profile**.
3. Under the **Financial Information** header, click the **Credit Cards** link.
4. In the **Credit Cards** window, click the **Add** button.
5. In the **Add Credit Card** window, make a note of the credit-card number, for use in later testing. Leave the automatically generated information as is.
6. Click **Add Credit Card**.

Generating a Credit Card Number to Test PayPal Account Optional

To obtain a test credit card number for testing PayPal Account Optional:

1. Select a buyer's test account, and click **Enter Sandbox Test Site**.
2. Navigate to **My Account > Profile**.
3. Under the **Financial Information** header, click the **Credit Cards** link.
4. Make a note of the credit-card number, for use in later testing.

Signing Up for Website Payments Pro

To sign up for Website Payments Pro, create a Business account, as described in "[Creating a Business Account](#)" on page 114."

To complete the application for Website Payments Pro, you must enter a Social Security Number. You can enter a Social Security Number in the following format:

111xxxxxx

where x is any digit.

NOTE: You cannot use a Social Security Number that is already recorded for another account in the Sandbox.

Testing PayPal Website Features

This chapter describes PayPal products features you can test in the Sandbox without PayPal APIs:

- **Website Payments with Buy Now Buttons** — Use the Sandbox to test accepting PayPal as a payment mechanism on a website.
- **Shopping Cart Purchases** — Use the Sandbox to test the purchase of multiple items in a single transaction, using a single payment.
- **Instant Payment Notification (IPN)** — Use the Sandbox to test IPN for updates and payment notifications.
- **Refunds** — Use the Sandbox to test refunding payments from a test buyer.
- **Subscriptions** — Use the Sandbox to test subscription buttons.

IMPORTANT: To execute test transactions on Sandbox, you need to complete a purchase as a test buyer with your buyer test account. Typically, you go through your website purchase flow as a buyer. Ensure that you execute your test on `www.sandbox.paypal.com` instead of `www.paypal.com`.

Website Payments with the “Buy Now” Button

You can use the Sandbox to familiarize yourself with the PayPal **Buy Now** button, with which you can associate PayPal with a specific item you sell on your website.

To create a test **Buy Now** button, follow these steps:

1. From the **Test Accounts** tab, select a business account and click **Enter Sandbox Test Site**.
2. Go to the **Merchant Services** tab.
3. Under the **Key Features** heading, select the **Buy Now Buttons** link to get to the Button Factory. You also can search the Help for “Button Factory.”
4. Follow the online instructions to create a Buy Now button. For details, see the [Website Payments Standard Integration Guide](#).
5. Copy and paste the code into your web page file wherever you want the button image to appear. Typically, the button should be located next to the description of the item or service. Your web page does not have to be published to your web server for you to check the button placement; it can be on you own local hard drive.

IMPORTANT: You must change the form action to redirect to the Sandbox, using the following URL:

```
https://www.sandbox.paypal.com/cgi-bin/webscr"
method="post"
```

Use the PayPal Help link to answer related questions, such as “How do I make a Buy Now button compatible with the shopping cart feature?” For general information, see

<https://www.paypal.com/pdn-item>. For general information about shopping-cart purchases, see <https://www.paypal.com/shoppingcart>. For general information about subscriptions, see <https://www.paypal.com/pdn-recurring>.

Encrypted Website Payments

The Sandbox also supports Encrypted Website Payments (EWP), as does the PayPal SDK console.

For information about EWP and how to use it, see *Website Payments Standard Integration Guide*.

For information about using the PayPal SDK console to generate EWP HTML, see *PayPal SDK Guide* for any supported platforms.

Testing Payments with Buy Now Button

To test the Buy Now button, your web page does not need to be published to your web server; it can reside on your local hard drive. You do need to be logged in to the Sandbox. Follow these steps:

1. Log in to <https://developer.paypal.com>, click the **Test Accounts** tab, select the desired test account, and click **Enter Sandbox Test Site**.
2. Open the HTML file containing the **Buy Now** Button.
3. Click the **Buy Now** Button.
4. Log in using your test buyer account.
5. Follow the on-screen instructions to complete your test payment.

Verifying a Test Payment

1. Log in to <https://developer.paypal.com> and click the **Test Email** tab. Your Sandbox inbox shows payment-confirmation email messages for the seller and buyer.
2. To further verify that the payment was successful:
 - Check your web server for IPN notifications related to the payment.
 - Launch the Sandbox as your test buyer or seller account, and navigate to **My Account > Overview** to see the transaction in your **Recent Activity**.

Handling Pending Transactions

Transactions typically are credited to your PayPal account instantly after the buyer completes the transaction; however, a buyer might select a payment method that is not completed instantly. In these cases, the transaction goes into a pending state, and the transaction is completed after a couple of days. The following sections describe how to set up pending-status transactions that can be either completed or canceled.

Creating a Pending Transaction

1. Log in to <https://developer.paypal.com>, click the **Test Accounts** tab, select a buyer (personal or premier) test account, and click **Enter Sandbox Test Site**.
2. Log in to your test buyer account and create a transaction, such as one created using a **Buy Now** button or by passing parameters in the URL, as in the following example:

```
https://www.sandbox.paypal.com/  
us/cgi-bin/webscr?cmd=_xclick&business=seller@domain.com
```

3. On the **Review Purchase Page**, click on the **Change** link under funding method.
4. Select **eCheck** as the funding method, and click **Continue**.
5. Click **Pay** to create the transaction.

To verify the creation of the transaction, see “[Verifying a Test Payment](#)” on page 119.

Completing or Canceling a Pending Transaction

1. In the buyer’s transactions log, click the **Details** link (in the Details column).
2. In the Transaction Detail window (shown below), there are two links to simulate actual bank clearing. These links appear only in the Sandbox, as shown below:
 - **Clear Transaction** — Click to complete the transaction.
 - **Fail Transaction** — Click to cancel the transaction.

The screenshot shows the PayPal Transaction Details page. At the top, there are navigation tabs: My Account, Send Money, Request Money, and Merchant Services. Below these are sub-tabs: Overview, Add Funds, History, and Profile. The main content area is titled 'Transaction Details' and shows an 'Add Funds from a Bank Account' transaction (ID #2T856487XV899364R). It includes two tables: 'Original Transaction' and 'Related Transaction'. The 'Original Transaction' table shows a payment to Gary McCue's Test Store for -\$10.00 USD on Apr. 25, 2008, with a status of 'Uncleared'. The 'Related Transaction' table shows the corresponding 'Add Funds from a Bank Account' for \$10.00 USD on the same date, also with a status of 'Uncleared'. Below the tables, it lists the Name (Bank Account), Total Amount (\$10.00 USD), Date (Apr. 25, 2008), Time (21:57:17 PDT), and Status (Uncleared, with an expected clearing date of Apr. 30, 2008). It also shows the Funding Type (eCheck) and Funding Source (Chase Manhattan Checking (Confirmed) xxxxxx9243). At the bottom right, there are links for 'Clear Transaction' and 'Fail Transaction', and a 'Return to Log' button.

Instant Payment Notification (IPN)

You can use the Sandbox to test Instant Payment Notification, such as the PayPal **Buy Now** button or reversals.

Setting up IPN in the Sandbox

For information about implementing IPN, see the following:

- Technical overview at <https://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/ipn-techview-outside>
- [Order Management Integration Guide](#)

test_ipn Variable. The Sandbox sets the `test_ipn` variable to a value of 1 in the HTTP response back to your IPN page. The purpose of this variable is to clearly differentiate between live and Sandbox IPN, so you can write your processing programs to work with either one. If the `test_ipn` variable is not in the HTTP response, you are working with Live PayPal.

To enable IPN for a test account, follow these steps:

1. Log in to <https://developer.paypal.com>, click the **Test Accounts** tab, select a test account, and click **Enter Sandbox Test Site**.
2. Click the **Profile** subtab.
3. Click the **Instant Payment Notification Preferences** link in the **Selling Preferences** column.
4. Click **Edit**.
5. Click the checkbox, and enter the URL where you want to receive your IPN notifications.
6. Click **Save**.
7. Install IPN on your web server. You might want to start with one of PayPal's source-code samples available at <https://www.paypal.com/ipn> under the **Code Samples** section. There are source-code samples for several programming languages and development environments. For details, see *Order Management Integration Guide*.

Verifying a Test Refund

To verify a test refund, you must have already made a test payment. Follow these steps:

1. Log in to <https://developer.paypal.com>.
2. Click the **Test Email** tab. Your Sandbox inbox shows refund-confirmation email messages for the seller and buyer.
3. To further verify that the refund was successful:
 - Check your Web server for IPN notifications related to the refund.
 - Launch the Sandbox as your test buyer or seller account, and navigate to **My Account > Overview** to see the transaction in your **Recent Activity**.

Transferring Funds to a Test Account

To transfer funds to a test account, follow these steps:

1. After logging into <https://developer.paypal.com>, select a test account and click **Enter Sandbox Test Site**.
2. Navigate to **My Account > Add Funds**.
3. Click the **Transfer funds from a Bank Account** link.

4. On the Add Funds by Electronic Funds Transfer page:
 - In the From drop-down list, select the bank account from which the funds are coming.
 - In the Amount box, enter the amount to transfer.
 - Click Continue.
5. On the resulting Add Funds Confirmation page, click **Submit**.
Navigate to **My Account > Overview**, to see that the transfer transaction is listed.

Clearing or Failing Test eCheck Transactions

When you use eCheck to transfer funds or send payments, the transaction appears as pending until you manually clear or fail it. Manual clearing is necessary only in the Sandbox.

To clear or fail test eCheck transactions, follow these steps:

1. In the transactions log, click the **Details** link (in the Details column).
2. In the Transaction Detail window, there are two links to simulate actual bank clearing. These links appear only in the Sandbox:
 - **Clear Transaction** — Click to complete the transaction.
 - **Fail Transaction** — Click to cancel the transaction.
3. Click **Return to Log** to see the transfer completed and the money in the Sandbox account. The **My Account > Overview** page opens.
4. Click the **View Limits** links on the **My Account > Overview** page, to see the spending limits for the current test account.

For an alternative example, see “[Completing or Canceling a Pending Transaction](#)” on [page 120](#).

Sending Funds to a Seller

To purchase goods or services, a PayPal user must send funds to a seller. In the PayPal Sandbox, you can simulate the actions of a buyer by manually initiating the payment of funds. You must use a Personal test account to represent the buyer.

To send funds from one test account to another, follow these steps::

1. Log in to <https://developer.paypal.com>, click the **Test Accounts** tab, select a test account, and click **Enter Sandbox Test Site**.
2. Navigate to the **Send Money** tab.
3. On the **Send Money** page, enter the email address (PayPal account name) for the test account in Recipient’s Email box.
4. In the Amount box, enter the amount to send to the seller’s test account.

5. In the **Currency** drop-down list, select the currency for the funds. (Note: **Auction** is not an option in the drop-down list.)
6. In the **Type** drop-down list, select the reason for sending the funds.
7. Enter text in the **Subject** box, if desired. This text is the subject of the email sent to the recipient about the transfer of funds.
8. Enter text in the **Note** memo box. This text appears in the body of the notification email.
9. Click **Continue**. This does not send the money; a confirmation step follows.
10. On the **Check Payment Details** page, review the transaction details for correctness. You can click **More Funding Options** to change the source of fund used for payment.
11. Click **Send Money**. This triggers the actual transfer of funds.
12. Your **Test Email** tab contains all the email messages sent to the test account sending the money and the test account receiving the money. See “[Test Email](#)” on page 110.
13. Log in as the seller test account and navigate to the **My Account > Overview** tab to see the transaction for the recipient’s account.

Billing A Customer

PayPal business users can bill another PayPal user for the purchase of goods or services. In PayPal terminology, the feature to bill a customer is called *Request Money*. In the PayPal Sandbox, you can manually initiate a request for funds from a test account. One test account is the seller; the other, the buyer.

To request funds from a buyer, follow these steps:

1. Log in to <https://developer.paypal.com>, click the **Test Accounts** tab, select a test account for which funds are requested, and click **Enter Sandbox Test Site**.
2. Navigate to the **Request Money** tab.
3. On the **Request Money** page, enter the email address (PayPal login name) for the test account being billed in the **Recipient’s Email** box.
4. In the **Amount** box, enter the billed amount.
5. In the **Currency** drop-down list, select the currency for the funds.
6. In the **Type** drop-down list, select the reason for the request for funds (billing). (Note: **Auction** is not an option in the drop-down list.)
7. Enter text in the **Subject** box. This text is the subject of the email sent to the recipient regarding the sent funds.
8. Enter text in the **Note** memo box. This text appears in the body of the notification email.
9. Click **Continue**.

10. On the **Request Money – Confirm** page, click **Request Money**. This triggers the actual request for funds.
11. Navigate to the **My Account > Overview** tab. The request for money should be listed.
12. Log in as the buyer, and navigate to the **My Account > Overview** tab to see the transaction for the buyer's test account. The transaction for the request for money appears on the **My Account > Overview** tab with **Pay** and **Cancel** buttons. Click **Pay**, and in the confirmation window, click **Send Money**. This completes the transfer of requested funds.

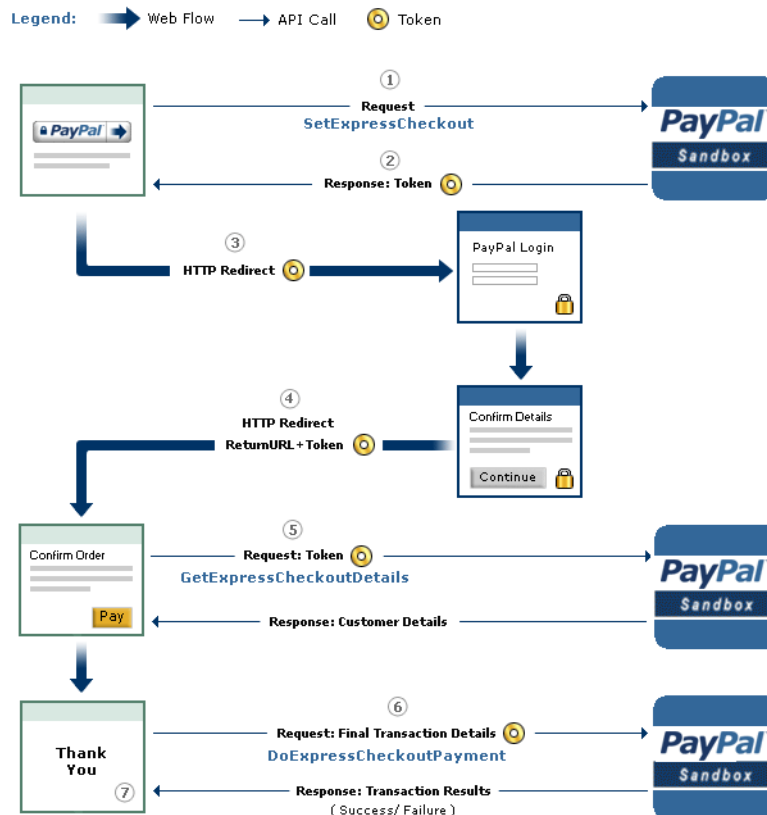
To view the email messages sent to both test accounts, select the **Test Email** tab. For details about your Sandbox email, see [“Test Email” on page 110](#).

Testing PayPal NVP APIs

This chapter describes how to test the Express Checkout name-value pair (NVP) API in the Sandbox. For more sophisticated examples, PayPal recommends you use the PayPal SDK that matches your environment, such as PHP or ASP. You also can use this chapter for ideas on how to establish a general testing procedure for PayPal APIs called from your site.

Testing Express Checkout

The following diagram shows the Express Checkout flow, which uses the Sandbox as the API server. The pages on the left represent your site.



NOTE: For information about Express Checkout, see *Express Checkout Integration Guide* and *PayPal NVP API Developer Guide and Reference*.

The following steps match the circled numbers in the diagram. To test Express Checkout, perform the actions in each step.

1. Invoke a form on your site that calls the `SetExpressCheckout` API on the Sandbox. To invoke the API, set form fields whose names match the NVP names of the fields you want to set, specify their corresponding values, then post the form to <https://api-3t.sandbox.paypal.com/nvp>, as shown below:

```
<form method=post action=https://api-3t.sandbox.paypal.com/nvp>
  <input type=hidden name=USER value= API_username>
  <input type=hidden name=PWD value= API_password>
  <input type=hidden name=SIGNATURE value= API_signature>
  <input type=hidden name=VERSION value=3.3>
  <input type=hidden name=PAYMENTACTION value=Authorization>
  <input name=AMT value=19.95>
```

```
<input type=hidden name=RETURNURL
  value=http://www.YourReturnURL.com>
<input type=hidden name=CANCELURL
  value=http://www.YourCancelURL.com>
<input type=submit name=METHOD value=SetExpressCheckout>
</form>
```

NOTE: The API username is a Sandbox business test account for which a signature exists. To obtain a signature, see the Test Certificates tab of the Sandbox.

2. PayPal responds with a message, like the one shown below. Note the status, which should include ACK set to Success, and a token that is used in subsequent steps.

```
TIMESTAMP=2007%2d04%2d05T23%3a23%3a07Z
&CORRELATIONID=63cdac0b67b50
&ACK=Success
&VERSION=3%3e300000
&BUILD=1%2e0006
&TOKEN=EC%2d1NK66318YB717835M
```

3. If the operation was successful, use the token and redirect your browser to the Sandbox, as follows:

```
https://www.sandbox.paypal.com/cgi-bin/webscr?cmd=_express-checkout
&token=EC-1NK66318YB717835M
```

NOTE: You may need to replace hexadecimal codes in the token with ASCII codes; for example, you may need to replace %2d in the token with a hyphen (-).

4. Log into the Sandbox and confirm details. You must log in to <https://developer.paypal.com> and select the test account that represents the buyer, not the *API_username* business test account that represents you as the merchant. Then click **Enter Sandbox Test Site**.

When you confirm, the Sandbox redirects your browser to the return URL you specified when calling SetExpressCheckout, as in the following example:

```
http://www.YourReturnURL.com/
?token=EC-1NK66318YB717835M&PayerID=7AKUSARZ7SAT8
```

5. Invoke a form on your site that calls the GetExpressCheckout API on the Sandbox:

```
<form method=post action=https://api-3t.sandbox.paypal.com/nvp>
  <input type=hidden name=USER value= API_username>
  <input type=hidden name=PWD value= API_password>
  <input type=hidden name=SIGNATURE value= API_signature>
  <input type=hidden name=VERSION value=3.3>
  <input name=TOKEN value=EC-1NK66318YB717835M>
  <input type=submit name=METHOD value=GetExpressCheckoutDetails>
</form>
```

If the operation was successful, the GetExpressCheckout API returns information about the payer, such as the following:

```
TIMESTAMP=2007%2d04%2d05T23%3a44%3a11Z
&CORRELATIONID=6b174e9bac3b3
&ACK=Success
&VERSION=3%3e300000
&BUILD=1%2e0006
&TOKEN=EC%2d1NK66318YB717835M
&EMAIL=YourSandboxBuyerAccountEmail
&PAYERID=7AKUSARZ7SAT8
&PAYERSTATUS=verified
&FIRSTNAME=...
&LASTNAME=...
&COUNTRYCODE=US
&BUSINESS=...
&SHIPTONAME=...
&SHIPTOSTREET=...
&SHIPTOCITY=...
&SHIPTOSTATE=CA
&SHIPTOCOUNTRYCODE=US
&SHIPTOCOUNTRYNAME=United%20States
&SHIPTOZIP=94666
&ADDRESSID=...
&ADDRESSSTATUS=Confirmed
```

6. Invoke a form on your site that calls the DoExpressCheckoutPayment API on the Sandbox:

```
<form method=post action=https://api-3t.sandbox.paypal.com/nvp>
  <input type=hidden name=USER value= API_username>
  <input type=hidden name=PWD value= API_password>
  <input type=hidden name=SIGNATURE value= API_signature>
  <input type=hidden name=VERSION value=3.3>
  <input type=hidden name=PAYMENTACTION value=Authorization>
  <input type=hidden name=PAYERID value=7AKUSARZ7SAT8>
  <input type=hidden name=TOKEN value=EC%2d1NK66318YB717835M>
  <input type=hidden name=AMT value= 19.95>
  <input type=submit name=METHOD value=DoExpressCheckoutPayment>
</form>
```


7. If the operation was successful, the response should include ACK set to `Success`, as follows:

```
TIMESTAMP=2007%2d04%2d05T23%3a30%3a16Z
&CORRELATIONID=333fb808bb23
&ACK=Success
&VERSION=3%3e300000
&BUILD=1%2e0006
&TOKEN=EC%2d1NK66318YB717835M
&TRANSACTIONID=043144440L487742J
&TRANSACTIONTYPE=expresscheckout
&PAYMENTTYPE=instant
&ORDERTIME=2007%2d04%2d05T23%3a30%3a14Z
&AMT=19%2e95
&CURRENCYCODE=USD
&TAXAMT=0%2e00
&PAYMENTSTATUS=Pending
&PENDINGREASON=authorization
&REASONCODE=None
```

Testing Error Conditions

In default operation, the Sandbox mimics the live PayPal site as closely as possible, which means an error can be replicated only by creating the exact conditions and sequence of events to raise an error. This *positive test* environment is well suited for testing logic that follows the typical error-free path; however, it can be difficult to raise error conditions and test logic to handle errors.

The Sandbox can be set to allow *negative testing*, which enables you to simulate an error. You can test against the following kinds of errors:

- Errors that result from calling a PayPal API.
- Address-verification and credit-card-validation errors that occur when using Virtual Terminal or calling `DoDirectPayment`.

IMPORTANT: Negative testing is available only for PayPal APIs Version 2.4 and later.

To raise an error condition, you set a value in a field passed to an API or a value in a field submitted to Virtual Terminal. The value triggers a specific error condition. Negative testing is available only in the Sandbox; you cannot force or simulate an error on the live site.

You must create a Business test account and enable negative testing; otherwise, setting a value in the API or transaction will not raise an error unless the error would be raised in the default positive-test environment. To enable negative testing, set **Test Mode** to **Enabled**.

The following screen shows two Business accounts. The first test account enables negative testing, and the second account disables negative testing.

The screenshot shows the PayPal Sandbox interface. At the top, there are navigation links: Home, Sandbox, Test Certificates, Email, Forums, and Help Center. Below this is the 'Sandbox' header. A paragraph explains that the Sandbox is a safe testing environment for PayPal payments and API calls, and it is a mirror of the real PayPal site except for real financial transactions. A 'Learn More...' link is provided. Below the text is a table titled 'Test Accounts' with a 'Create Account' link. The table has columns for User, Type, CountryCode, Country, Balance, Confirmed, Verified, and Test Mode. There are two rows of test accounts, one with a green status icon and one with a blue status icon.

User	Type	CountryCode	Country	Balance	Confirmed	Verified	Test Mode
	Business	us	U.S.	0.00 USD	Yes	Unverified	Enabled
	Business	us	U.S.	0.00 USD	Yes	Unverified	Disabled

To test Virtual Terminal, you must set risk controls for address verification and credit-card security, respectively, to **Decline** or **Accept and Report** depending on the kind of negative testing you want to perform. If you do not set the appropriate risk controls, default processing occurs, which is to accept the transaction.

Severe error conditions, such as bad arguments or invalid login, preempt negative testing because the error cannot be handled by negative or positive testing. In these cases, the error condition for positive testing is raised, regardless of whether the account was enabled for negative testing.

API Testing

For APIs, you trigger an error condition by setting a field to the value of the error you want to trigger. The value you specify depends on the kind of field:

- For amount-related fields, specify a value as a number with two digits to the right of the decimal point; for example, 107.55 triggers PayPal API error 10755.
- For other kinds of fields, specify the actual PayPal API error; for example, 10755 triggers PP API error 10755.

Table 9.2 identifies the API, the NVP name or SOAP element of the field that triggers the error, and a description of how to set the value in the field.

TABLE 9.2 API Fields That Trigger Error Conditions

API Name	NVP Field Name	SOAP Element	Description
RefundTransaction	AMT	Amount	Specify the error code to trigger as all digits in a number with two digits to the right of the decimal point; e.g., 107.55 triggers PayPal API error code 10755.
GetTransaction Details	TRANSACTIONID	TransactionID	Specify the error code to trigger as all digits in the field; e.g., 10755 triggers PayPal API error code 10755.
TransactionSearch	INVNUM	InvoiceID	Specify the error code to trigger as all digits in the field; e.g., 10755 triggers PayPal API error code 10755.

TABLE 9.2 API Fields That Trigger Error Conditions (Continued)

API Name	NVP Field Name	SOAP Element	Description
DoDirectPayment	AMT	OrderTotal	Specify the error code to trigger as all digits in a number with two digits to the right of the decimal point; e.g., 107.55 triggers PayPal API error code 10755.
SetExpressCheckout	MAXAMT	MaxAmount	Specify the error code to trigger as all digits in a number with two digits to the right of the decimal point; e.g., 107.55 triggers PayPal API error code 10755.
GetExpressCheckout Details	TOKEN	Token	Specify the error code to trigger as all digits in the field; e.g., a token value of 10755 triggers PayPal API error code 10755.
DoExpressCheckout	TOKEN	Token	Specify the error code to trigger as all digits in the field; e.g., a token value of 10755 triggers PayPal API error code 10755.
DoCapture	AMT	Amount	Specify the error code to trigger as all digits in a number with two digits to the right of the decimal point; e.g., 106.23 triggers PayPal API error code 10623.
DoVoid	AUTHORIZATIONID	AuthorizationID	Specify the error code to trigger as all digits in the field; e.g., an ID of 10623 triggers PayPal API error code 10623.
DoReauthorization	AMT	Amount	Specify the error code to trigger as all digits in a number with two digits to the right of the decimal point; e.g., 106.23 triggers PayPal API error code 10623.
DoAuthorization	AMT	Amount	Specify the error code to trigger as all digits in a number with two digits to the right of the decimal point; e.g., 106.23 triggers PayPal API error code 10623.
MassPay	EMAILSUBJECT	EmailSubject	Specify the error code to trigger as all digits in the field; e.g., a subject of 10755 triggers PayPal API error code 10755.
BillUser	AMT	Amount	Specify the error code to trigger as all digits in a number with two digits to the right of the decimal point; e.g., 107.55 triggers PP API error code 10755.

TABLE 9.2 API Fields That Trigger Error Conditions (Continued)

API Name	NVP Field Name	SOAP Element	Description
BAUpdate Version 2.4	MPID	MpID	Specify the error code to trigger as all digits in the field; e.g., an ID of 10755 triggers PayPal API error code 10755.
BAUpdate Version 3.0	REFERENCEID	ReferenceID	Specify the error code to trigger as all digits in the field; e.g., an ID of 10755 triggers PayPal API error code 10755.
AddressVerify	—	—	Not supported for negative testing.

NOTE: If the trigger value is not a valid error code for the API being tested, positive testing occurs for the request, which might result in another error occurring.

Negative Testing Using an Amount-Related Trigger Field

The following example sets up testing for error 10623 for DoAuthorization, in which the error code is specified in the AMT field:

```
METHOD=DoAuthorization
&TRANSACTIONID=0-1GU0288989807143B&
AMT=106.23&
TRANSACTIONENTITY=Order&
VERSION=3.3&
USER=username&
PWD=password&
SIGNATURE=signature
```

The request invokes the following response:

```
TIMESTAMP=2007%2d04%2d04T03%3a10%3a19Z&
CORRELATIONID=447d121150529&
ACK=Failure&
L_ERRORCODE0=10623&
L_SHORTMESSAGE0=Maximum%20number%20of%20authorization%20allowed%20for%20the%20order%20is%20reached%2e&
L_LONGMESSAGE0=Maximum%20number%20of%20authorization%20allowed%20for%20the%20order%20is%20reached%2e&
L_SEVERITYCODE0=Error&
VERSION=3%3e400000&
BUILD=1%2e0006
```

Negative Testing Using a Non-Amount Trigger Field

The following example sets up testing for error 10603 for DoVoid, in which the error code is specified in the AUTHORIZATIONID field:

```
METHOD=DoVoid&  
AUTHORIZATIONID=10603&  
VERSION=3.3&  
USER=username&  
PWD=password&  
SIGNATURE=signature
```

The request invokes the following response:

```
TIMESTAMP=2007%2d04%2d04T03%3a10%3a22Z&  
CORRELATIONID=51b0c5054dee6&  
ACK=Failure&  
L_ERRORCODE0=10603&  
L_SHORTMESSAGE0=The%20buyer%20is%20restricted%2e&  
L_LONGMESSAGE0=The%20buyer%20account%20is%20restricted%2e&  
L_SEVERITYCODE0=Error  
&VERSION=3%3e400000&  
BUILD=1%2e0006
```

Negative Testing With Multiple Messages

The following example sets up testing for error 10009 for RefundTransaction, which returns 14 possible error message sets:

```
METHOD=RefundTransaction&  
TRANSACTIONID=asdf&  
REFUNDTYPE=Partial&  
AMT=100.09&  
VERSION=3.3&  
USER=username&  
PWD=password&  
SIGNATURE=signature
```

The request invokes the following response:

```

TIMESTAMP=2007%2d04%2d04T03%3a10%3a23Z&
CORRELATIONID=81ccc18eaec49&
ACK=Failure&
L_ERRORCODE0=10009&
L_SHORTMESSAGE0=Transaction%20refused&
L_LONGMESSAGE0=You%20can%20not%20refund%20this%20type%20of%20transaction&
L_SEVERITYCODE0=Error&
L_ERRORCODE1=10009&
L_SHORTMESSAGE1=Transaction%20refused&
L_LONGMESSAGE1=You%20are%20over%20the%20time%20limit%20to%20perform%20a%20r
efund%20on%20this%20transaction&
L_SEVERITYCODE1=Error&
L_ERRORCODE2=10009&
L_SHORTMESSAGE2=Transaction%20refused&
L_LONGMESSAGE2=Account%20is%20restricted&
L_SEVERITYCODE2=Error&
...
L_ERRORCODE13=10009&
L_SHORTMESSAGE13=Transaction%20refused&
L_LONGMESSAGE13=The%20partial%20refund%20amount%20must%20be%20less%20than%2
0or%20equal%20to%20the%20remaining%20amount&
L_SEVERITYCODE13=Error&
VERSION=3%3e400000&
BUILD=1%2e0006

```

Testing Using AVS Codes

You can simulate address verification by triggering an AVS error code when you call `DoDirectPayment` or use Virtual Terminal. To specify a code, place `AVS_code` in the `NVP_SHIPTOSTREET` field or the `Street1` SOAP element when you call `DoDirectPayment`, where `code` is an AVS code. Alternately, enter `AVS_code` in Address Line 1 when using Virtual Terminal. For example, if you set `123 AVS_A Street` in the `NVP_SHIPTOSTREET` field, AVS code A is set.

NOTE: `AVS_code` is case sensitive; all characters must be uppercase. For example, `AVS_A` is a valid trigger, but `avs_a` is not.

Table 9.3 identifies valid AVS codes, corresponding triggers, and description of the error conditions.

TABLE 9.3 AVS Error Conditions and Triggers

AVS Code	Trigger	Description of Error
A	AVS_A	The address matches, but no zip code is specified. This results in an error if the “Partial Address Match” risk control is set.
B	AVS_B	The international address matches, but no zip code is specified. This results in an error if the “Partial Address Match” risk control is set.
D	AVS_D	Exact match (no error). The international address and postal code match.

TABLE 9.3 AVS Error Conditions and Triggers (Continued)

AVS Code	Trigger	Description of Error
F	AVS_F	Exact match (no error). The UK address and postal code match.
P	AVS_P	The postal code matches, but no address is specified. This results in an error if the “Partial Address Match” risk control is set.
W	AVS_W	The 9-digit zip code matches, but no address is specified. This results in an error if the “Partial Address Match” risk control is set.
X	AVS_X	Exact match (no error). The complete address and 9-digit zip code match.
Y	AVS_Y	Exact match (no error). The complete address and 5-digit zip code match.
Z	AVS_Z	The 5-digit zip code matches, but no address is specified. This results in an error if the “Partial Address Match” risk control is set.
N	AVS_N	There is no address information. This results in an error if the “No Address Match” risk control is set.
C	AVS_C	There is no address information for an international address. This results in an error if the “No Address Match” risk control is set.
E	AVS_E	Not allowed for MOTO (internet/phone) transactions.
I	AVS_I	Service is unavailable internationally. This results in an error if the “Service Unavailable/Unsupported” risk control is set.
G	AVS_G	Service is unavailable globally. This results in an error if the “Service Unavailable/Unsupported” risk control is set.
R	AVS_R	Retry. This results in an error if the “Service Unavailable/Unsupported” risk control is set.
S	AVS_S	Service is not supported. This results in an error if the “Service Unavailable/Unsupported” risk control is set.
U	AVS_U	Service is unavailable. This results in an error if the “Service Unavailable/Unsupported” risk control is set.

NOTE: The specified AVS code is set, regardless of whether a PP API error code is set. If no AVS code is specified or the AVS risk control is not specified, AVS code X is returned.

Testing an AVS Code Using Virtual Terminal

Consider an example of testing for AVS code A using Virtual Terminal. You enter `AVS_A` in the **Address Line 1** field:

Virtual Terminal - Order Entry Form

* indicates required field [hide optional fields](#)

Order Details

*Currency: U.S. Dollars

*Net Order Amount: \$5

*Shipping: \$0 Apply tax to shipping

*Tax Rate: 0.000 %

Tax Amount: \$0.00

Total: \$5.00

*Transaction Type: Auth

Item Name/Service:

Order Number:

Billing Information - Please enter the following information **exactly** as it appears on the customer's credit card statement.

Country: United States

First Name:

Last Name:

*Card Type: Visa

*Card Number: 4011238251268087

*Expiration Date: 01 2008

*Card Security Code: 000 (On the back of your card, locate the final 3 digit number) [What's this? Using Amex?](#)

Address Line 1: 123 AVS_A St.

Address Line 2:

City:

State:

ZIP Code:

Email Address:

Home Telephone:

Shipping Address

No shipping address required

Use the same above billing address as the shipping address

Enter a separate shipping address

When you try to process the transaction, the following AVS error message appears from Virtual Terminal:

PayPal [Log Out](#) | [Security Center](#)

Virtual Terminal - Order Entry Form

10555: This transaction cannot be processed.

- Filter Decline
- Processor Response Code: 0000.
- AVS: A - Address only match.
- CVV: M - Pass.
- Reference # F10CC2B1F2B3A

Testing an AVS Code Using DoDirectPayment

The following example sets up testing for AVS code A and error code 10755 in DoDirectPayment, for which AVS code A indicates no zip code is specified and results in an error if the “Partial Address Match” risk control is set, regardless of whether other errors occur:

```
METHOD=DoDirectPayment&
CREDITCARDTYPE=VISA&
ACCT=4683075410516684&
EXPDATE=112007&
CVV2=808&
AMT=107.55&
FIRSTNAME=Designer&
LASTNAME=Fotos&
IPADDRESS=255.55.167.002&
STREET=1234%20AVS_A%20Street&
CITY=San%20Jose&
STATE=CA&
COUNTRY=United%20States&
ZIP=95110&
COUNTRYCODE=US&
SHIPTONAME=Louise%20P.%20Flowerchild&
SHIPTOSTREET=1234%20Easy%20Street&
SHIPTOSTREET2=Apt%2022%20bis&
SHIPTOCITY=New%20Orleans&
SHIPTOSTATE=LA&
SHIPTOCOUNTRY=US&
SHIPTOZIP=70114&
PAYMENTACTION=Authorization&
FIZBIN=foo&
VERSION=3.3&
USER=username&
PWD=password&
SIGNATURE=Aq9tJJ3ndj7r32JgX.qAzqOoC1JJAM7erWun-CUZYFDtxffpKWU4ERQG
```

The request invokes the following response:

```
TIMESTAMP=2007%2d04%2d04T03%3a35%3a10Z&
CORRELATIONID=a7cbf2d4d83dc&
ACK=Failure&
L_ERRORCODE0=10555&
L_SHORTMESSAGE0=Filter%20Decline&
L_LONGMESSAGE0=This%20transaction%20cannot%20be%20processed%2e&
L_SEVERITYCODE0=Error&
L_ERRORCODE1=10755&
L_SHORTMESSAGE1=Unsupported%20Currency%2e&
L_LONGMESSAGE1=This%20transaction%20cannot%20be%20processed%20due%20to%20an%20unsupported%20currency%2e&
L_SEVERITYCODE1=Error&
VERSION=3%3e400000&
BUILD=1%2e0006
```

Testing Using CVV Codes

You can simulate credit-card validation by triggering a CVV error code when you call `DoDirectPayment` or use Virtual Terminal. To specify a CVV code, place a trigger value in the `NVP CVV2` field or the `CVV2 SOAP` element when you call `DoDirectPayment`, or enter the trigger in **Card Security Code** when using Virtual Terminal.

[Table 9.4](#) identifies valid CVV codes, corresponding triggers, and descriptions of the error conditions.

TABLE 9.4 CVV Error Conditions and Triggers

CVV Code	Trigger	Description of Error
M	115	CVV2 matches (no error).
N	116	CVV2 does not match.
U	125	Service unavailable.
S	123	Service not supported.
P	120	Transaction not processed.
X	130	No response.

NOTE: The specified CVV2 code is set, regardless of whether a PP API error code is set. If no CVV2 code is specified, M is returned. Virtual Terminal displays the CVV2 error only if the risk control blocks the payment.

Testing a CVV Code Using Virtual Terminal

Consider an example of testing for CVV code N using Virtual Terminal. You enter 116 in the **Card Security Code** field:

The screenshot shows the PayPal Virtual Terminal interface. At the top, there are navigation links for 'My Account', 'Send Money', 'Request Money', and 'Merchant Services'. Below this is a sub-navigation bar with 'Dashboard', 'Add Funds', 'History', and 'Profile'. The main heading is 'Virtual Terminal - Order Entry Form'. A note indicates that fields with an asterisk are required. The 'Order Details' section includes:

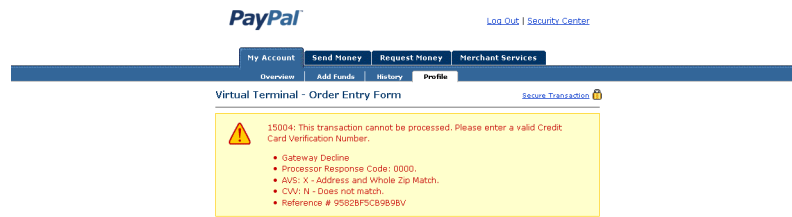
- Currency: U.S. Dollar
- Net Order Amount: \$5
- Shipping: \$0
- Tax Rate: 0.00%
- Tax Amount: \$0.00
- Total: \$5.00
- Transaction Type: Auth

 The 'Billing Information' section contains:

- Card Type: Visa
- Card Number: 4011230251268007
- Expiration Date: 01/2008
- Card Security Code: 116

 The Card Security Code field is highlighted in red. At the bottom, there are buttons for 'Review Transaction' and 'Cancel'.

When you try to process the transaction, the following CVV error message appears from Virtual Terminal:



NOTE: Other errors are also reported in addition to CVV code N.

Testing a CVV Code Using DoDirectPayment

The following example sets up testing for CCV code N in DoDirectPayment, which indicates a mismatch in the card-validation code:

```
METHOD=DoDirectPayment&
CREDITCARDTYPE=VISA&
ACCT=4683075410516684&
EXPDATE=112007&
CVV2=116&
AMT=1.55&
FIRSTNAME=Designer&
LASTNAME=Fotos&
IPADDRESS=255.55.167.002&
STREET=1234%20Easy%20Street&
CITY=San%20Jose&
STATE=CA&
COUNTRY=United%20States&
ZIP=95110&
COUNTRYCODE=US&
SHIPTONAME=Louise%20P.%20Flowerchild&
SHIPTOSTREET=1234%20Easy%20Street&
SHIPTOSTREET2=Apt%20222%20bis&
SHIPTOCITY=New%20Orleans&
SHIPTOSTATE=LA&
SHIPTOCOUNTRY=US&
SHIPTOZIP=70114&
PAYMENTACTION=Authorization&
FIZBIN=foo&
VERSION=3.3&
USER=username&
PWD=password&
SIGNATURE=signature
```

The request invokes the following response:

```
TIMESTAMP=2007%2d04%2d04T03%3a35%3a12Z&
CORRELATIONID=2499856319532&
ACK=Failure&
L_ERRORCODE0=15004&
L_SHORTMESSAGE0=Gateway%20Decline&
L_LONGMESSAGE0=This%20transaction%20cannot%20be%20processed%2e%20Please%20e
nter%20a%20valid%20Credit%20Card%20Verification%20Number%2e&
L_SEVERITYCODE0=Error&
VERSION=3%3e400000&
BUILD=1%2e0006
```

Testing Recurring Payments

On the live site, a billing cycle repeats after the actual specified time elapses; for example, a one-month billing cycle takes one month to occur. You can simulate the elapsed time for a billing cycle in the Sandbox when testing a recurring payments profile, in which case the actual elapsed time is reduced. This is useful when you want to simulate a billing cycle without waiting for the actual time to elapse.

To reduce the actual elapsed time, specify `Day` as the period. When you specify `Day`, the billing cycle occurs every n minutes in the Sandbox, where n represents the frequency. For example, if you specify 1 for the billing frequency and `Day` for the period when executing the `CreateRecurringPaymentsProfile` API, the billing cycle occurs every minute when testing in the Sandbox.

IMPORTANT: Reducing the elapsed time works only if the period is `Day`; other values do not change the actual elapsed time.

Consider a scenario in which you want to simulate a one-month billing cycle after a three-month trial, without waiting four months. In the Sandbox, you could specify the following NVP parameters:

```
...&TRIALBILLINGPERIOD=Day&TRIALBILLINGFREQUENCY=3
...&BILLINGPERIOD=Day&BILLINGFREQUENCY=1...
```

In the Sandbox, the trial billing period would take approximately three minutes and the regular billing cycle would occur approximately every minute. When you are ready to go live, you would change the trial billing period and the billing period to `Month`.

Review Questions

Answers to review questions are in [Appendix A, “Answers to Review Questions.”](#)

1. True or false: Sandbox email messages use the same email system as live PayPal email messages.
2. What variable does the Sandbox use to differentiate between live PayPal and Sandbox IPN?
3. What two pieces of information must be changed in the application code when moving the application from the Sandbox to live PayPal?
4. True or false: An application does not have to be published to a web server before a tester can test a **Buy Now** button.
5. Which of the following applies to the passwords you can specify for your Sandbox accounts?
 - (a) They must be the same as the password for your Developer Central account.
 - (b) They can be the same for all your test accounts, to make testing easier.
 - (c) They must begin with “sb”.
 - (d) They must be unique for each Sandbox account.

A

Answers to Review Questions

Chapter 1

1. Indicate if each statement is True (T) or False (F).

- T The most critical step in establishing an online store is ensuring that you can accept customer payments for single or repeated transactions.
- F Correct answer: According to Cybersource Corp., businesses lost nearly \$2.8 billion USD to online fraud in 2005, up from \$2.8 billion USD in 2004.
- T The payment processing network connects buyers, sellers, and banks to enable the secure and reliable execution of online transactions.
- T By providing affordable payment connections among merchants, customers, and financial networks, PayPal's solutions take advantage of the latest technical resources to streamline transactions, while helping to prevent fraud.

2. Match each participant in the payment processing network to the role they perform.

Response	Participant	Role Performed
3	Merchant	1. The holder of the payment instrument.
1	Customer	2. A financial institution that provides credit card services in concert with credit card associations such as Visa and MasterCard.
6	Customer Issuing Bank	3. Someone who sells goods or services.
5	Acquiring Bank	4. A large data center that processes credit card transactions and settles funds for merchants.
2	Credit Card Association	5. An institution that provides merchant accounts required to enable online card authorization and payment processing.
4	Processor	6. The institution providing the customer's credit card.

3. The following steps describe the payment authorization process. Indicate the correct order of the steps by placing the step number to the left of each description.
- 4 Processor routes information to bank that issued customer's credit card.
 - 2 Merchant's website receives customer information and sends it to payment processing service.
 - 7 Processing service sends results to merchant.
 - 8 Merchant decides to accept or reject purchase.
 - 1 Customer decides to purchase online and inputs credit card information.
 - 6 Processor routes transaction results to payment processing service.
 - 3 Processing service routes information to processor.
 - 5 Issuing bank sends authorization (or declination) to processor.
4. The following steps describe the payment processing settlement process. Indicate the correct order of the steps by placing the step number to the left of each description.
- 5 Acquiring bank credits merchant's bank account.
 - 1 Merchant informs the payment processing service to settle transactions.
 - 3 Processor checks the information, and forwards settled transaction information to the card association and card-issuing bank.
 - 6 Issuing bank includes merchant's charge on customer's credit card account.
 - 4 Transactions are settled to the card issuers and funds move between the acquiring bank and issuing bank. Funds received for these transactions are sent to the merchant's bank account.
 - 2 Payment processing service sends transactions to processor.
5. Finding a reliable, secure, and flexible payment processing solution is critical. What features should a payment processing solution offer? (Select all that apply.)
- X Backed by an established, trustworthy company
 - X Comply with Payment Card Industry (PCI) Data Security Standard
 - Store customer financial information in plain sight
 - X Authorize credit cards in real time
 - Based on a network that provides near real-time credit card transactions
 - X Scale rapidly and seamlessly as transaction volume increases
 - X Offer upgrade options to accommodate future growth
 - X Provide recurrent billing payment for service

6. Match each PayPal solution to the service it offers.

Response	PayPal Product	Service Description
4	Website Payments Pro	1. Lets you send customers email invoices that they can pay on PayPal. This simple solution does not require you to have a shopping cart or an internet merchant account.
7	Website Payments Standard	2. A gateway that provides a secure connection between your online store and your internet merchant account. Scalable and fully customizable, this solution is recommended for merchants who require peak site performance and direct control over payment functionality on their site. Merchants using this service can enhance the customer experience by allowing shoppers to complete the checkout process without ever leaving your site.
2	Payflow Pro	3. Allows merchants to put the PayPal logo on their own website to accept PayPal as an alternative payment source, in addition to credit cards such as MasterCard® or Visa®.
5	Payflow Link	4. An all-in-one payment solution that allows customers to shop and pay on your site. You can accept credit cards directly on your site and get the features of a merchant account and gateway through a single provider at a lower cost.
1	PayPal Email Payments	5. A gateway that provides a secure connection between your online store and your internet merchant account. This service is designed for merchants who require a simple solution to selling on the web. In order to use this service, you need to add only a small piece of HTML code that will link your customers to order forms hosted by PayPal.
6	PayPal Virtual Terminal	6. Provides your business with the same functionality as a stand-alone credit card-processing terminal, but allows you to accept credit card payments by phone, fax, and email.
3	PayPal as an Additional Payment Option	7. Lets customers shop on your website and pay on PayPal. It offers a pay-per-use model with no set-up or monthly fees. It includes shipping and tax calculators, reporting tools to measure your business, and support for international currencies.

7. Select the PayPal payment processing solutions that enable a customer to checkout on the merchant's website.
- X Website Payments Pro
 - Website Payments Standard
 - X Payflo Pro
 - Payflow Link
 - Email Payments
 - Virtual Terminal
 - PayPal as an Additional Payment Option
8. Select the PayPal payment processing solutions that require API or HTML technical skills to develop payment processing applications.
- X Website Payments Pro
 - X Website Payments Standard
 - X Payflo Pro
 - X Payflow Link
 - Email Payments
 - Virtual Terminal
 - X PayPal as an Additional Payment Option

Chapter 2

1. Indicate if each statement is True (T) or False (F).
- T Every merchant is at risk for fraud.
 - F Correct answer: Internet fraud is more difficult to detect than in the brick-and-mortar world.)
 - T Credit card associations hold merchants liable for fraudulent transactions because the credit card is not physically present during online purchases.
 - T American Express, Diners Club, Discover Card, JCB, MasterCard International, and Visa U.S.A. have adopted the Payment Card Industry (PCI) Data Security Standard developed to protect account and transaction information of cardholders.
 - F Correct answer: According to Gartner Group estimates, merchants reject an estimated 5% of all transactions out of suspicion of fraud, while only 2% of transactions are actually fraudulent. The result is a significant amount of lost sales (up to 3% of sales volume) in an attempt to reduce fraud risk.

2. List the four most common fraud-related risks facing online merchants.
 - Consumer identity theft
 - Merchant identify theft
 - Accessing payment networks
 - Chargebacks
3. Match each participant in the payment processing network to the role they perform.

Response	Risk Category	Potential Risk Description
7	Merchants with vulnerable security defenses	1. Fraud attempts are higher for merchants who advertise heavily or are in the news because criminals know that merchants who experience high transaction volumes have less time to defend against fraud.
1	High-visibility merchants	2. It is difficult to validate the address or identity of foreign buyers, and it is more difficult to investigate and prosecute fraudulent activity from an overseas source.
3	High-ticket goods that are easily resold	3. These items, including luxury goods, computers, and other electronic equipment, are most attractive to criminals.
6	Goods that can be downloaded from the internet	4. Criminals know that you have limited time for fraud protection when sales volumes are high. That's why internet fraud triples in the fourth quarter.
2	International customer base	5. Criminals watch for special offers. They know that you have limited time for fraud protection measures when sales volumes are high.
4	Heavy proportion of fourth quarter sales	6. The purchase of these goods doesn't require physical address information, making it easier for criminals to disguise a fraudulent transaction.
5	Special promotions	7. Criminals take advantage of sophisticated spidering techniques to identify merchants with network vulnerabilities, and can then break into your network to steal account access information for hijacking or merchant takeovers.

4. List two actions you can take to ensure that each transaction your website accepts and processes is valid. (Select any two.)
 - Authenticate buyer when possible.
 - Screen orders for fraud patterns.
 - Review suspicious transactions.

5. Fill in the blanks to complete the following statements.

PayPal leverages the Secure Sockets Layer (SSL) protocol, which provides crucial online identity and security to help establish trust between parties involved in e-commerce transactions.

Using SSL with an encryption key length of 128 bits (the highest level commercially available), PayPal automatically encrypts your confidential information in transit from your computer to ours.

PayPal's servers sit behind a monitored electronic firewall and are not connected directly to the internet, so your private information is available only to authorized computers.

6. List three ways to reduce chargebacks. (Select any three.)

- Provide realistic delivery time estimates and use tracking that shows proof that the items were received.
- Describe the sale item in as much detail as possible. Include clear images and measurements so that customers have a good understanding of what they're getting.
- Make sure you clearly disclose the total cost to customers up front: the price, taxes, shipping costs, etc.
- Provide customers with a way to contact you should they have a problem. Often a simple email exchange or phone call clears up a misunderstanding instantly.
- Respond promptly and courteously to customer inquiries.

7. List the five areas you should cover in your website disclosure policy.

- Business description
- Privacy policy
- Shipping policy
- Return policy
- Contact information

8. The left column in the table lists the PCI data security standards. The right column contains a list of requirements. Indicate which requirements meet each standard. (Note: Each standard has one or more requirements.)

Response	Standards	Requirements
8, 11	Build and Maintain a Secure Network	1. Restrict physical access to cardholder data.
4, 5	Protect Cardholder Data	2. Regularly test security systems and processes.
3, 7	Maintain a Vulnerability Management Program	3. Develop and maintain secure systems and applications.
1, 6, 12	Implement Strong-Access Control Measures	4. Encrypt transmission of cardholder data and sensitive information across public networks.
2, 9	Regularly Monitor and Test Networks	5. Protect stored data.
10	Maintain an Information Security Policy	6. Assign a unique ID to each person with computer access.
		7. Use and regularly update antivirus software.
		8. Do not use vendor-supplied defaults for system passwords and other security parameters.
		9. Track and monitor all access to network resources and cardholder data.
		10. Maintain a policy that addresses information security.
		11. Install and maintain a firewall configuration to protect data.
		12. Restrict access to data by business need-to-know.

9. Define the following standard antifraud features included with each PayPal Payflow Gateway solution.

- Card security code. A three- or four-digit number printed on the physical card, which a customer provides to you at checkout.
- Address verification system (AVS). A system that verifies the credit card holder's personal address and billing information.

10. Indicate if each statement is True (T) or False (F).

- T PayPal's Basic Fraud Protection Service is the ideal solution for merchants who process low transaction volumes through a Payflow payment gateway, while the Advanced Fraud Protection Service is essential for businesses processing medium-to-high transaction volumes.
- T Both the Basic Fraud Protection Service and the Advanced Fraud Protection Service catch common fraud warnings like high dollar amounts, high quantities, and shipping/billing address mismatch.
- T To support automatic rejection lists and automatic acceptance lists, you need to upgrade to PayPal's Advanced Fraud Protection Service.
- F Correct answer: The PayPal Account Monitoring service is an upgrade option that provides full-time protection to keep an eye on suspicious activity related to credits and refunds.

Chapter 3

1. The following steps describe the getting started with account setup process. Indicate the correct order of the steps by placing the step number to the left of each description.
 - 2 Set up an internet merchant account, if you don't already have one.
 - 5 Customize your payment processing service with additional services.
 - 1 Choose payment processing services.
 - 4 Use the PayPal APIs to implement payment processing on the merchant website.
 - 3 Enroll in the selected PayPal services.
2. What information do you need to set up an internet merchant account?

To set up an internet merchant account, have the following information available:

 - Account/business owner's name, address, and email
 - Business name and address
 - Customer service information
3. How many days should you allow to set up an internet merchant account?

Three to five business days
4. Match each PayPal service that provides fraud protection to its description.

Response	PayPal Product	Service Description
3	Fraud Protection Services	1. Provides your customers with a secure and convenient payment flow because they don't have to re-enter information already stored in their PayPal account.
1	Express Checkout	2. A fast, cost-effective way to accept repeat payments for installment plans, monthly fees, or subscription-based services.
2	Recurring Billing Service	3. Provides simple automated credit card fraud screening to enterprise-grade perimeter security services to save you time and money while protecting your business.

5. What is the purpose of the PayPal Sandbox?

The *PayPal Sandbox* is a self-contained environment in which developers can prototype and test PayPal applications. Before moving any PayPal-based application into production, test the application in the Sandbox to ensure that it functions properly.

Chapter 4

1. False. API credentials must be included with every request sent to the PayPal server.
2. True.

Chapter 5

1. An ampersand (&).
2. True.
3. The METHOD parameter.
4. True.

Chapter 6

1. From the value that was sent to PayPal in the DoExpressCheckoutPayment request.
2. \$10,000 USD, in any currency.
3. Three hours.
4. On the shopping cart page, aligned with any other checkout buttons.
5. TAXAMT is required if a value for L_TAXAMT*n* is specified.

Chapter 7

1. True.
2. It is determined by the Merchant Account settings.

Chapter 8

1. Up to 115% of the originally authorized amount (up to \$75 USD).
 2. False.
 3. If REFUNDTYPE is Full, do not set AMT.
 4. True.
 5. No.
 6. A *complaint* occurs when a customer registers a complaint about a payment to PayPal. A *chargeback* occurs when a customer registers a complaint with the credit card company.
-

Chapter 9

1. False.
2. `test_ipn`
3. The server address and the developer's API credentials.
4. True.
5. (b) They can be the same for all your test accounts, to make testing easier.

B

General Reference Information

This appendix contains information that may be valuable when using the PayPal NVP APIs.

ShippingAddress Parameter

The `ShippingAddress` parameter is optionally used in a `SetExpressCheckout` or `DoExpressCheckoutPayment` request in Express Checkout, and in a `DoDirectPayment` request in Direct Payment.

TABLE B.1 *ShippingAddress*

Parameter	Description	Required?
SHIPTONAME	Person's name associated with this shipping address. Character length and limitations: 32 single-byte characters	Yes
SHIPTOSTREET	First street address. Character length and limitations: 100 single-byte characters	Yes
SHIPTOCITY	Name of city. Character length and limitations: 40 single-byte characters	Yes
SHIPTOSTATE	State or province. Character length and limitations: 40 single-byte characters	Yes
SHIPTOCOUNTRYCODE	Country code. Character limit: Two single-byte characters NOTE: A complete list of country codes is available in the <i>PayPal Name-Value Pair API Developer Guide and Reference</i> .	Yes
SHIPTOZIP	U.S. ZIP code or other country-specific postal code. Character length and limitations: 20 single-byte characters	Yes
SHIPTOSTREET2	Second street address. Character length and limitations: 100 single-byte characters	No
PHONENUM	Phone number. Character length and limitations: 20 single-byte characters	No

PayPal-Supported Transactional Currencies

Table B.2 lists the currencies supported by PayPal for use in transactions.

TABLE B.2 PayPal-Supported Currencies and Currency Codes for Transactions

ISO-4217 Code	Currency
AUD	Australian Dollar
CAD	Canadian Dollar
CHF	Swiss Franc
CZK	Czech Koruna
DKK	Danish Krone
EUR	Euro
GBP	Pound Sterling
HKD	Hong Kong Dollar
HUF	Hungarian Forint
JPY	Japanese Yen
NOK	Norwegian Krone
NZD	New Zealand Dollar
PLN	Polish Zlotny
SEK	Swedish Krona
SGD	Singapore Dollar
USD	U.S. Dollar

AVS Response Codes

Table B.3 lists the AVS response codes for U.S. credit cards (Visa, MasterCard, Discover, and American Express).

TABLE B.3 AVS Response Codes

AVS Code	Meaning	Matched Details
A	Address	Address only (no ZIP)
B	International “A”	Address only (no ZIP)
C	International “N”	None NOTE: The transaction is declined.
D	International “X”	Address and Postal Code
E	Not allowed for MOTO (internet/phone) transactions	Not applicable NOTE: The transaction is declined.
F	UK-specific “X”	Address and postal code
G	Global Unavailable	Not applicable
I	International Unavailable	Not applicable
N	No	None NOTE: The transaction is declined.
P	Postal (International “Z”)	Postal code only (no address)
R	Retry	Not applicable
S	Service not supported	Not applicable
U	Unavailable	Not applicable
W	Whole ZIP	Nine-digit ZIP code (no address)
X	Exact match	Address and nine-digit ZIP code
Y	Yes	Address and five-digit ZIP code
Z	Zip	Five-digit ZIP code (no address)
All others	Error	Not applicable

CVV2 Response Codes

Table B.4 lists the CVV2 response codes for U.S. credit cards (Visa, MasterCard, Discover, and American Express).

TABLE B.4 CVV2 Response Codes

CVV2 Code	Meaning	Matched Details
M	Match	CVV2
N	No match	None
P	Not processed	Not applicable
S	Service not supported	Not applicable
U	Service not available	Not applicable
X	No response	Not applicable



Glossary

A

Address Verification System (AVS) — A system used to verify the identity of a credit card holder.

API certificate — A file (downloaded from PayPal) that includes a key and certificate that identify a developer. An API certificate must be installed on a web server; therefore, it is an option only if the developer has full control of the web server.

API credentials — A set of data that uniquely identifies a developer to the PayPal API server. The credentials are attached to every API call.

API password — This is automatically generated and assigned by PayPal. It is a randomly generated string of 16 characters.

API signature — An encrypted string value included with each API call.

API username — This is assigned by PayPal. Although the API username is based on the email address used to set up the credentials, it is *not* the same as the email address used to log in to the PayPal website

Authorization & capture APIs — A PayPal payment solution that separates the authorization for a purchase from the actual capture of the funds. This is useful for merchants who have a delayed order fulfillment process or who need to modify the original authorization amount due to order changes.

C

Case — A claim registered with PayPal by a buyer who has a dispute with a merchant.

Chargeback — A transaction in which a customer requests a refund from the credit card company, and the credit card company bills the merchant. Chargebacks often occur as a result of fraudulent transactions or disputes in which the customer was not properly credited after a return.

Card Verification Value (CVV2) — A three- or four-digit value printed on a credit card but not encoded on the card's magnetic strip. This value provides security against credit card fraud in transactions in which the merchant does not directly handle the credit card, such as e-commerce transactions.

I

Instant Payment Notification (IPN) — A PayPal solution that provides merchants with immediate notification and confirmation of PayPal payments received.

P

PayPal Direct Payment API — An API that enables merchants to accept credit card payments directly on their website. PayPal remains invisible, so that the merchant controls the customer experience.

PayPal Express Checkout — An API that allows PayPal account holders to check out fast with saved information, and enables merchants to gain incremental sales from the growing base of PayPal users.

R

Redirect — To automatically induce a web browser to go to a new location.

Request-response model — A message exchange pattern in which an application sends a request message to a server, and the server executes the request and returns a message in response to the application.

S

Sandbox — A self-contained environment in which developers can prototype and test PayPal applications.

T

Token — A parameter used in Express Checkout to identify a transaction.

W

Website Payments Pro — An all-in-one payment solution that includes the Direct Payment API and Express Checkout.

I

Index

A

- acquiring bank 12
- adding a bank account 115
- address verification system (AVS) 34
- address verification testing 134
- Advanced Fraud Protection Service 35
- API certificate 48
 - and Sandbox 50
 - encrypting 49
 - generating 49
 - installing 49
- API credentials 56
 - definition 47
 - required security parameters 50
- API server for Sandbox 105, 106
- API signature 48
 - protecting 48
- API testing 130
- Authorization & Capture
 - and Direct Payment 76, 85
 - and Express Checkout 76, 85, 87
 - authorization period 88
 - authorization process 87
 - best practices 93
 - definition 87
 - DoCapture API
 - request 88
 - response 89
 - DoReauthorization API
 - request 92
 - response 92
 - DoVoid API
 - request 91
 - response 92
- authorizations 12

B

- bank account
 - adding 115
 - for Canadian test accounts 116

- for German test accounts 116
 - for UK test accounts 116
- Bank Account Number 116
- Basic Fraud Protection Service 34
- billing a customer 124
- BSB Number 116
- Business account 114
- business description 30
- Buy Now 118
- Buyer Authentication 34

C

- Canadian bank account info 116
- card security code 34
- cases 103
- cash theft 25
- chargebacks 26, 103
- chargebacks, reduction 29
- consumer identity theft 25
- contact information 31
- credit card associations 12
- credit card validation testing 138
- customer 12
- customer issuing bank 12

D

- Direct Marketing Association (DMA) 33
- Direct Payment 79
 - and Authorization & Capture 76, 85
 - DoDirectPayment API
 - request 80
 - response 84
 - workflow 79
- disclosure and compliance resources 33
- disclosure policy 30
- disputes 103
- DoCapture
 - request 88
 - response 89

DoDirectPayment

- request 80
- response 84

DoExpressCheckoutPayment

- request 68
- response 71

DoReauthorization

- request 92
- response 92

DoVoid

- request 91
- response 92

E**eCheck** 123**email**

- live
 - payment notification 99

email in Sandbox 111**Email Payments** 17**errors, testing** 129**Express Checkout** 44, 59

- and Authorization & Capture 76, 85, 87
- button placement 73

DoExpressCheckoutPayment API

- request 68
- response 71

GetExpressCheckoutDetails API

- request 66
- response 66

SetExpressCheckout API

- and updating shipping address 76
- request 62
- response 65
- workflow 60

F**Federal Trade Commission** 33**fraud detection in Sandbox** 106**Fraud Protection Services** 14, 28, 34, 44**G****German bank account info** 116**GetExpressCheckoutDetails**

request 66

response 66

getting started 43**GetTransactionDetails**

- request 99
- response 99

I**identify theft** 25**Instant Payment Notification (IPN)**

- activating 100
- processing 101
- shared secret validation 101
- validating 101
- workflow 100

Instant Payment Notification. See *IPN*.**Institution Number** 116**internet fraud** 23, 25, 26**internet merchant account** 43**IPN**

- ipn_test variable 121
- technical overview 121
- testing in Sandbox 121

L**liability** 24**M****MasterCard** 33**merchant** 12**merchant identity theft** 25**N****name-value pair**

- API servers 58
- definition 53
- format 54
- integrating with PayPal 53
- request 54, 56
- request-response model 54
- response 54, 57
- samples 53

name-value pair (NVP) APIs 125

negative testing 129

O

OpenSSL 49
Order Review page 76

P

Payflow Gateway products 15
Payflow Link 14, 15, 17, 43
Payflow Pro 14, 15, 17, 43
paying 123
Payment Card Industry (PCI) Data Security Standard 13, 24, 31
payment processing authorization 12
payment processing network 11
payment processing service 12
payment processing services 43
payment processing settlement 13
PayPal as an Additional Payment Option 16
PayPal Email Payments 15
PayPal Sandbox 44
PayPal Virtual Terminal 15
pending transactions 120
Personal account 112
positive test 129
Privacy Planner 33
privacy policy 30
processor 12
product theft 25

R

Recurring Billing Service 44
Recurring Billing Service for Payflow 14
recurring payments, testing 140
refunds 93
 RefundTransaction API
 request 94
 response 94
RefundTransaction
 request 94
 response 94
reporting tools 100
request 54, 56
Request Money testing 124

request-response model 54
 URL-encoding 55
response 54, 57
 errors 57
return policy 31

S

Sandbox 44
 API server for 105, 106
 email 111
search
 GetTransactionDetails API
 request 99
 response 99
 TransactionSearch API
 request 95
 response 98
Secure 29
secure HTTP (HTTPS) 58
Secure Sockets Layer (SSL) protocol 29
Send Money 123
SetExpressCheckout
 and updating shipping address 76
 request 62
 response 65
settlements 12
shared secret validation 101
shipping policy 30
Social Security Number for Website Payments Pro 117
sort code for Canada, Germany, and UK 116
source code samples
 for IPN 122

T

test accounts 111
test email 111
test_ipn 121
testing
 address verification 134
 APIs 130
 billing a customer 124
 Buy Now 119
 credit card validation 138
 eCheck 123
 IPN 121

- negative 129
- paying 123
- Send Money 123
- verifying a payment 119
- verifying a refund 122
- Website Payments 118
- testing recurring payments 140
- TransactionSearch
 - request 95
 - response 98
- Transit Number 116

U

- UK bank account info 116
- URL-encoding 55

V

- Virtual Terminal 17
- Visa 33

W

- Website Payments 118
- Website Payments Pro 14, 17, 43, 111, 117
- Website Payments Standard 14, 15, 17, 43