PayPal

Fraud Prevention

What Every Merchant Should Know About Internet Fraud

PayPal Business Guide

PayPal Business Guide – Fraud Prevention

Notice of Non-Liability

PayPal, Inc. and the authors assume no liability for errors or omissions, or for damages, resulting from the use of this guide or the information contained in this guide.

Table of Contents

Introduction

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. As an internet merchant, 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.

PayPal has put together this guide to help you better understand fraud and what you can do to prevent it. The guide covers the following topics:

- 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
- Let customers know that your store is safe for purchases
- Reducing 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
- Save time and money while protecting your business with PayPal® Fraud Protection Services

Why Every Merchant Should Be Concerned About Internet Fraud

Every merchant is at risk for fraud. So it just makes good business sense to be aware and informed of your exposure and how to protect your business.

As a merchant 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.

"Since going live with PayPal Fraud Protection Services, we have saved significant time and, more importantly, $10,000 in just three weeks by stopping fraudulent orders. We used to be poorly protected, but now we not only have the armor but also the ability to control the level of protection. It's a great feeling."

Robert Meyer
Director of
Internet Services
Anaconda Sports

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 merchant concern. Running efficient security operations that don't impact your bottom line is essential.

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 you, 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

"PayPal helps make chargebacks a very minimal part of our business."

Lonny Paul
TigerDirect.com

Plus, 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

Yes, there is a greater element of risk in the online world, but there is also an element of reward if you properly manage that risk. 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 your virtual cash register by stealing merchant account access information and impersonating you in order to issue credits or payments to themselves.

"We were scared to take international orders because we thought they would all be chargebacks. But we don't have fear anymore. PayPal Fraud Protection Services have saved us thousands and thousands of dollars."

Shelly Baldwin
Payments Manager
Initio

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:

1. Didn't receive the item ordered
2. Didn't receive the item believed to be ordered
3. Had his or her credit card stolen and used by the thief
4. 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.

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.
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.

Let Customers Know That Your Store Is Safe for Online Purchasing

To turn your online storefront into a thriving business, you must first win your customers' trust. Many web users are still uncomfortable sending credit card numbers over the internet. In traditional brick-and-mortar businesses, consumers accept the risks of using credit cards because they can see and touch the merchandise and make judgments about the store. On the internet, without those physical cues, it's more difficult for customers to assess the safety of your business. Merchants who can prove the security of their website will gain the loyalty – and business – of consumers, which can help significantly increase revenue.

"PayPal is committed to making sure that the transactions are secure. This really seems to reassure buyers."

Kurt Denke
BlueJeansCable.com

Reducing Your 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, your payment gateway account, and your 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 – giving you 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

"PayPal was one of the few companies that would take the security completely off our shoulders, and more importantly, help protect our customers."

Tim Schuler
RotoWire.com

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.

We help your business stay secure.

- PayPal's industry-leading loss rate is less than 0.5%*
- We protect sensitive information using state-of-the-art encryption, so your data is not available to anyone

We help you keep out fraud.

- Our proprietary risk models help detect and predict fraudulent transactions – before they affect your business*
- We use industry-recognized address verification system (AVS) and card security code checks to thwart identity theft
- We employ patent-pending bank account verification as an additional level of authentication. Verification gives you more information about the people with whom you transact through PayPal, so you can make more informed decisions.*

We help shield you from liability.

- PayPal fights chargebacks to help your business avoid losses*
- We go even further to protect you against chargebacks with PayPal's Seller Protection Policy for qualified transactions. Your business can be protected from liability at no additional cost.*

* Only applies to Website Payments Pro, Website Payments Standard, and Email Payments.

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

Save Time and Money While Protecting Your Business With 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 – time and resources that are better served in building and growing your business.

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.

We've made choosing the right PayPal Fraud Protection Services package for your business easy. And it's simple to upgrade, so you only buy what you need, when you need it.

"With PayPal, the amount of fraud is much lower, which saves me time and money."

Dan Pritchett
LowCarbChocolates.com

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.

Compare 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.	✓	✓
Unusual Order Filters Catch common fraud warnings like high dollar amounts, high quantities, and shipping/billing address mismatch.	✓	✓
High-Risk Payment Filters Catch suspicious transactions like rapid repeat buying from an internet address.	✓	✓
High-Risk Address Filters Check for suspect ZIP codes and freight forwarders plus IP address.	✓	✓
Automatic Rejection Lists Help protect you business from known offenders.		✓
Automatic Acceptance Lists Keep good customers buying by automatically accepting their payments.		✓
High-Risk International Filters Identify risky international payments.		✓
Additional Risk Filters Get more tools to catch warning signs like rapid card use, risky banks, and tighter address validations.		✓
Custom Filter Wizard Customize new rules that match your specific business needs.		✓
Operations Security Identify vulnerabilities and list fixes with a security audit from Qualys.	✓	✓

PayPal Fraud Protection Services Upgrade Options

Account Monitoring

Whether you have Basic or Advanced Fraud Protection, you can now get extra, around-the-clock protection with Account Monitoring. This 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

Now you can easily get 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.** Easily 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.

"In the past, we were challenged with fraudulent activity. Solutions like PayPal Fraud Protection Services help us reduce processing time, allowing us to get more timely updates on sales, payment processing, and inventory. Additionally, it's cutting down on customer wait times when purchasing online."

Dale Knox
Controller
Dallas Cowboys Wholesale

What You Need to Get Started

In three easy steps a merchant can acquire everything needed to begin accepting online purchases.

1. Choose a payment processing service.

- 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. PayPal's 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 PayPal Payflow Pro or Payflow Link, PayPal provides the option to apply for an internet merchant account with our preferred merchant account provider.

3. Customize your payment processing service with additional services.

Protect your business and your 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 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 your customers:

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

Offer your 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 us at **1-888-847-2747**, send us an email at paymentsales@paypal.com, or visit the PayPal Merchant Services section of the PayPal website at www.paypal.com.