3 Ways to Fight Fraud and Get More Secure in Online Commerce
# Table of contents

**Introduction** ........................................................................................................................... 3  
**Building Block 1: Know thy fraud** ....................................................................................... 4  
  Nine common types of online fraud ............................................................................... 4  
    Identity theft .................................................................................................................... 4  
    Phishing attacks .............................................................................................................. 4  
    Reshipping ....................................................................................................................... 4  
    Affiliate fraud ................................................................................................................... 4  
    Scripted and botnet attacks ............................................................................................ 5  
    Card testing ....................................................................................................................... 5  
    Account takeover .............................................................................................................. 5  
    Friendly fraud ................................................................................................................... 5  
    Triangulation fraud ......................................................................................................... 6  
**How do modern fraud rings operate?** ............................................................................ 7  
  They’re highly organized .................................................................................................... 7  
  They defy blacklists ............................................................................................................ 7  
  They’re flexible and constantly adapting ........................................................................ 8  
**Building Block 2: Build a solid, secure foundation with PCI DSS compliance** ........... 9  
**PCI DSS FAQs** .................................................................................................................... 9  
**Getting started** ............................................................................................................... 11  
  STEP 1: Determine your level ............................................................................................. 11  
  STEP 2: Complete the SAQ ................................................................................................. 11  
  STEP 3: Complete a vulnerability scan ............................................................................ 11  
**Building Block 3: Add data security and fraud mitigation solutions** ........................ 12  
**Tokenization** ..................................................................................................................... 12  
**Address verification service (AVS)** .............................................................................. 14  
**Card security checks** ...................................................................................................... 15  
**Fraud filters and fraud scoring** ..................................................................................... 16  
**Conclusion** .......................................................................................................................... 18
Introduction

When your business sells goods and services online, the opportunity for fraud can skyrocket. From stolen identities to intricate card scams, fraudsters are only becoming more adept at stealing personal information and using it for their own illegal purposes.

Despite advances in card security features, many are designed to fight fraud at the point of sale (POS) and don’t provide the same protection in online commerce. For example, EMV cards (also known as chip cards) use cryptographic technology to ensure that fraudulent cards aren’t accepted at in-store payment terminals. Unfortunately, the technology that powers EMV doesn’t extend to online commerce. And fraudsters are taking notice.

While not as obvious as EMV chips on payment cards, there are data security solutions designed to protect payment transactions and personal information online. Using these solutions in conjunction with the Payment Card Industry Data Security Standard (PCI DSS) can help your business create an environment for safer, more secure online commerce. While it’s impossible to stop the threat of online fraud in its entirety, it is possible to protect your business from the financial and reputational risks associated with it.

And that’s what this Vantiv eBook is all about. In it, we’ll:

- Identify nine common types of online fraud and investigate how modern crime rings operate
- Discuss the role of PCI DSS compliance and identify key considerations for your online business
- Outline specific data security solutions that your online business can use to fight fraud, including tokenization, address verification service, card security checks, and advanced fraud filters/scoring
Building Block 1: Know thy fraud

Nine common types of online fraud

Fraud is a big term. So what do we mean when we talk about fraud in online commerce? Let’s take a closer look at nine common types of online fraud.

1. IDENTITY THEFT

Identity theft is the most common type of fraud and occurs when personal information – name, address, email, phone, payment card information – is stolen and the fraudster assumes that identity as his or her own. They can use this information to get credit or purchase items using another person’s account. According to a recent study by Javelin Strategy & Research, more than 13 million Americans had their identities stolen in 2015, which amounted to a loss of $15 billion for consumers, banks, and others.¹

→ TIP: Be sure to keep all of your technology and software updated. When security vulnerabilities are spotted, the compromised software rushes to get a patch together and hackers scramble to capitalize on those holes. So quit putting off those updates – it’s the easiest way to secure sensitive data.

2. PHISHING ATTACKS

Phishing attacks are popular ways to steal information, which employ falsified communications (websites, emails, text messages, etc.) that encourage people to give up their personal data. Other methods for capturing this information include browser Trojans, key loggers, and system breaches. Fraudsters can then use this stolen information to create fake identities, make illegal purchases, and gain unauthorized access to the victims’ online accounts.

3. RESHIPPING

In order to successfully commit payment fraud online, criminals have to be creative in how they thwart controls that are in place to prevent them from doing so. One such way is through reshipping fraud. It begins when merchandise is purchased online using stolen payment card information. Orders are then typically shipped to an American address where accomplices are paid to reship the goods to new buyers in the United States or foreign countries. Doing so facilitates fulfillment of the original order by using a domestic address so as not to raise red flags about the ultimate destination of the package.

4. AFFILIATE FRAUD

Merchants often use marketing affiliates to help promote their businesses and increase online sales. However, this opens a new door for fraudsters to commit their nefarious deeds. Using stolen card information, affiliates can initiate fraudulent transactions to collect commissions for sales that were falsified with stolen payment information. Merchants pay these affiliates for sales performance and are later on the hook for subsequent chargebacks that occur.

SCRIPTED AND BOTNET ATTACKS

Bots are secret programs that are installed on computers without the owners knowing. This happens through the use of computer worms, viruses, and other forms of malware. Once a bot is successfully installed on a computer, the fraudster can control that computer and “see” all of the personal information that’s entered into it, including payment information. When many computers are infected with bots, they become a botnet and the opportunity for stealing credit card information multiplies as the network grows.

CARD TESTING

Card testing allows criminals to “test” stolen credit card information by placing small ticket orders on legitimate websites. For example, fraudsters can take payment card information they’ve obtained illegally and make small purchases (typically under $5.00) to ensure that the low-dollar transactions are authorized. If these transactions are approved, they know they have the correct information to make bigger and more expensive purchases. As an added bonus for the crooks, card testing often goes unnoticed by legitimate card holders because the transaction amounts are so low that they might not raise any red flags.

ACCOUNT TAKEOVER

Account takeover is exactly how it sounds. It occurs when criminals take over users’ accounts by stealing usernames, passwords, account numbers, and/or social security numbers. By posing as the true account owners, fraudsters can make purchases without raising suspicion. While these unauthorized transactions usually occur within a short period of time before the real account owners realize what’s going on, it’s often enough time to create significant damage for both consumers and merchants. In addition, users often share passwords across multiple websites which makes all merchants easier targets when one has a breach.

FRIENDLY FRAUD

Despite its name, friendly fraud (also known as chargeback fraud) isn’t so friendly to you, the merchant. It happens when a customer makes a legitimate charge on his or her payment card but then disputes the charge for a refund. If the customer is successful in reporting the purchase as fraud the merchant may face fines, fee increases from the card brands, and possibly even a permanent suspension of their processing account. There are two types of friendly fraud that merchants should understand: intentional and accidental.

Intentional friendly fraud usually involves a customer who purchases an item, receives it, and then claims that they didn’t place the order or never received it. This usually results in an automatic customer refund. The merchant must then gather evidence to dispute the chargeback and prove that the transaction was approved by the cardholder.
Accidental friendly fraud occurs when a customer reports an incorrect charge because they aren’t aware that another authorized user on the account made the purchase. It also happens when the customer doesn’t recognize the information on their billing statement because it doesn’t match the business’s name. Unlike intentional friendly fraud, accidental friendly fraud is more easily resolved. Often all it takes is a phone call to the customer to review and explain the transaction.

→ TIP: Make sure your company’s billing descriptor easily identifies your business on card statements. Use a company name or brand the customer will recognize and include a toll-free telephone number. If your customer doesn’t remember the purchase, they will generally call the number in the descriptor before contacting the card issuer. Confirm your descriptors regularly to ensure that the information isn’t being truncated.

9 TRIANGULATION FRAUD

As the name suggests, triangulation fraud schemes are comprised of three distinct interaction points. First, there’s a fake seller listing items on online marketplaces. These listings usually offer unbelievable deals on popular goods, making the bargains hard for shoppers to resist. Customers enter their payment information to purchase the goods at the discounted price.

The second part of the scheme is when the payment information entered by the customer is used to “make good” on the original purchase. Meaning, the stolen card information is used at a legitimate merchant to fulfill the order that the customer is expecting. Because the original order is fulfilled, it often takes longer to recognize triangulation fraud schemes and for cardholders to report the unauthorized transactions.

The third and final part is when the merchant fulfilling the order is duped into accepting fraudulent payment card information. It’s extremely difficult for a merchant to trace a transaction back to the original fraudster and prevent further fraudulent orders from being placed.

→ TIP: There are specific types of suspicious activity that can raise red flags of potential fraud. For example, be on alert if your online store receives several orders from a single IP address but uses different payment cards. This pattern could indicate that a single fraudster is using multiple stolen cards to make purchases from your business. Also look for remarkably large orders, especially when the purchaser requests next-day shipping. Such a large purchase, shipped as soon as possible, could be a sign that the customer wants to receive the order as quickly as possible before the card theft is discovered and halted.
How do modern fraud rings operate?

Now that we’ve discussed the major types of online fraud, it’s important to learn more about the traits of modern fraudsters and their organized crime rings. Here are three things to know: they’re highly organized, they defy blacklists, and they’re flexible and constantly adapting.

Let’s discuss all three in detail.

THEY’RE HIGHLY ORGANIZED

The idea of a hacker working alone in a darkened room is not the reality for most fraudsters. They tend to be highly organized enterprises, with well-defined operational processes and where each contributor plays a specific role. Some are specialists, while others oversee and manage the entire operation. Some are part of discrete, vertically-integrated organizations, while others provide specialized services “for hire.” The complexity of the “stolen card supply chain” continues to mature as thieves find new efficiencies to increase revenue, reduce cost, and minimize risk.

→ TIP: How can you counter the attacks of well-organized individuals and crime syndicates? Be just as organized, or more so, when it comes to your business operations and fraud mitigation strategy. Partner with other merchants, your payment processor, and other solution providers to tap into a shared database of intelligence to detect and deter fraud.

THEY DEFY BLACKLISTS

When it comes to payments fraud, it’s easy to conjure images of shady, overseas black-market operators. All your business needs to do is blacklist shipments to well-known offending nations and you’ll be safe, right?

Not so fast.

These foreign marketplaces are often supplied by lengthy and sophisticated schemes that allow merchants to mistakenly assume they are dealing with buyers in the United States. This can leave merchants with a false sense of security that they’re serving their local markets.

The same is true for other types of blacklisted sources, including email, IP addresses, and payment cards. Remember that fraudsters are adept at identifying and overcoming these obstacles to continue to defraud merchants and consumers. Therefore, blacklists should be used but carefully managed.

→ TIP: While fraud impacts every business and industry uniquely, it’s a mistake to assume that you truly know who your customer is. Fraudsters employ a variety of methods to cloak their true identities and locations. Use in-house and third-party fraud tools to scrutinize every transaction.
THEY’RE FLEXIBLE AND CONSTANTLY ADAPTING

Countering the schemes of payment criminals can be far more effective if you know your enemy. However, fraudsters are proficient at engineering their way around tripwires and honeypots that are set for them. And as commerce continues to evolve, so do the criminals.

For example, the 2015 holiday shopping season saw more and more fraudsters taking advantage of new in-store pick up options to carry out their attacks. Merchants should consider in-store pick up the ultimate form of expedited shipping, allowing fraudsters to receive their stolen goods in minutes rather than days. The bad guys often hire fellow criminals to pick up goods already paid for online with stolen payment cards. Merchants with highly evolved billing and shipping address verification controls are unable to use these anti-fraud tools for newer, more seamless shopping methods.

This example underscores a larger point; namely, a set-it-and-forget-it approach to fraud prevention isn’t nearly enough. Anyone engaged in online commerce needs a fraud strategy that’s as flexible and adaptable as the criminals they intend to block. As your business changes to offer new services and conveniences (for example, in-store pick up or a gift card program), fraudsters’ methods and tactics will change to take advantage of new opportunities as well.
Building Block 2: Build a solid, secure foundation with PCI DSS compliance

So where do you begin to block the fraud ecosystem from profiting off of your organization? One of the most important steps toward better security is adopting the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS are a set of industry tools and measurements to help ensure the safe handling of sensitive information. PCI DSS was developed to safeguard the personal information of cardholders while in the possession or use of merchants, payment processors, and other entities that store, process, or transmit payment card information.

Understanding the basics of PCI DSS, defining your merchant level, and understanding your validation requirements are critical. Failure to adhere to these requirements may result in significant fines and potential cancellation of merchant accounts by the card brands.

Here’s a quick overview of PCI DSS and how to get started.

PCI DSS FAQs

To whom does PCI DSS apply?

The PCI DSS compliance program applies to all entities that store, process, or transmit cardholder data.

What are the benefits?

It’s good business practice to adhere to PCI DSS and protect cardholder information. Additionally, the card brands (MasterCard, Visa, and Discover) may impose significant fines on merchants that aren’t compliant.

What is cardholder data?

Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc.

How is a PCI DSS level determined?

A PCI DSS level is determined by annual transaction volume. The volume calculation is based on the gross number of Visa, MasterCard, Discover, American Express, or JCB transactions processed within your merchant account.

Can compliance requirements change?

Yes. As your business’s transaction volume changes, and as association and industry rules change, your compliance requirements may change as well. It’s your business’s responsibility to be aware of the data security requirements that apply to your current situation.
What if your business doesn’t store cardholder data?

Even if your business doesn’t store cardholder data, PCI DSS still applies to the environment that transmits or processes cardholder data. This includes any service providers that store, process, or transmit cardholder data on your business’s behalf.

Are there fines associated with non-compliance?

Yes. Visa, MasterCard, and Discover may impose fines on their member banking institutions when merchants don’t comply with PCI DSS. Your business is contractually obligated to indemnify and reimburse your acquirer for such fines, which could be significant.

Are there fines if cardholder data is compromised?

Yes. If cardholder data that you are responsible for is compromised, your business may be subject to the following liabilities and fines:

- Potential fines of up to $500,000 (at the discretion of Visa, MasterCard, Discover, or other card brands)
- All fraud losses incurred from the use of the compromised account numbers from the date of the compromise forward
- The cost of reissuing cards associated with the compromise
- The cost of any additional fraud prevention/detection activities required by the card bands (i.e., a forensic audit) or the costs incurred by credit card issuers associated with the compromise (i.e., additional monitoring of system for fraudulent activity)
# Getting started

## STEP 1: DETERMINE YOUR LEVEL

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Criteria</th>
<th>Onsite Security Assessment</th>
<th>Self-Assessment Questionnaire</th>
<th>Network Vulnerability Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>At least 6 million transactions annually from any acceptance channel for Visa, MasterCard, or Discover</td>
<td>Required Annually</td>
<td>N/A</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>2</td>
<td>1 million to 6 million transactions annually from any acceptance channel for Visa, MasterCard, or Discover</td>
<td>At Merchant Discretion*</td>
<td>Required Annually*</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>3</td>
<td>20K to 1 million eCommerce transactions annually from any acceptance channel for Visa, MasterCard, or Discover</td>
<td>N/A</td>
<td>Required Annually</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>4</td>
<td>Less than 20K eCommerce annually or less than 1 million transactions from any acceptance channel for Visa, MasterCard, or Discover</td>
<td>N/A</td>
<td>Required Annually</td>
<td>Required Quarterly</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Provider Level</th>
<th>Criteria</th>
<th>Onsite Security Assessment</th>
<th>Self-Assessment Questionnaire</th>
<th>Network Vulnerability Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>More than 300K transactions annually for Visa or MasterCard</td>
<td>Required Annually</td>
<td>N/A</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>2</td>
<td>300K or less transactions annually for Visa or MasterCard</td>
<td>N/A</td>
<td>Required Annually (SAQ – D)</td>
<td>Required Quarterly</td>
</tr>
</tbody>
</table>

*Effective 30 June 2012, Level 2 merchants that choose to complete an annual Self-Assessment Questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC-offered merchant training programs and pass any associated PCI SSC accreditation program annually in order to continue the option of self-assessment for compliance validation. Alternatively, Level 2 merchants may, at their own discretion, complete an annual onsite assessment conducted by a PCI SSC-approved QSA rather than complete an annual Self-Assessment Questionnaire.

## STEP 2: COMPLETE THE SAQ

Identify your validation type, determine which Self-Assessment Questionnaire is appropriate for your business, and complete the SAQ. [View and download the SAQs](https://www.pcisecuritystandards.org/).

## STEP 3: COMPLETE A VULNERABILITY SCAN

Complete and obtain evidence of passing a vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV). It is required for Validation Type 4 and 5 – those merchants with external-facing IP addresses. You can find a Qualified Security Assessor and Approved Scanning Vendor (ASV) at: [https://www.pcisecuritystandards.org/](https://www.pcisecuritystandards.org/).
Building Block 3: Add data security and fraud mitigation solutions

PCI DSS compliance is just the beginning. There are advanced data security solutions that can add extra protection and help prevent fraud in your online payments acceptance program. They include tokenization, address verification service, card security checks, and fraud filters/scoring. We’ll explore each of them here.

Tokenization

Tokenization is one of the most simple and straightforward ways to protect your customers against the negative effects of a data breach. So what is tokenization and how can it make your online business more secure?

Tokenization allows you to remove sensitive cardholder information from your systems.

Tokenization lets you substitute a credit, debit, prepaid, or checking account number stored on your system with a string of numbers known as a token. Each token is specific to your business and useless to anyone else who might try to use it, so you can store it without concern.

Implementing and using tokens should be seamless.

Implementing and using tokens should be completely transparent to both your business and its customers. Tokens should be card-based, not transaction-based, so they fit easily into your existing systems, including OMS, billing, and ERP systems.

Tokenization can reduce your scope of PCI DSS compliance.

Tokenization can reduce the scope of your systems that fall under PCI DSS compliance requirements, thereby reducing the costs and man hours associated with the auditing process. This can extend beyond your production system to include your failover system, disaster recovery (“backup”) system, and testing environments.

You can get your data back.

If at any time you want your cardholder information returned to you, your tokenization provider should be able to provide it in a secure, PCI DSS-compliant manner in its entirety. Therefore, you never lose ownership of your vital customer information.
What should your business look for in a tokenization solution?

1. **Service Compatibility** - your tokens should be fully-compatible with all standard processing transactions, including authorizations, deposits, sales, refunds, and chargebacks.

2. **Format Preservation** - with format preservation, each token is the same length as the card number it replaces (generally 15 or 16 digits) so you don’t have to modify your systems.

3. **End-to-end Protection** - look for a solution that replaces the personal account number (PAN) with a token prior to the authorization, at the initial capture of the card, whether that’s in an online shopping cart, in your mobile app, or at a POS terminal. By tokenizing at the point of card entry, you eliminate the risk of theft while the data is “in transit” and minimize your PCI DSS scope, which can reduce your annual compliance cost burden.

4. **Channel Neutral** - your customers expect to be able to use the same card on file whether online, via a mobile app, or at a mobile POS. Make sure your provider offers an “omni-token” solution so you can adapt accordingly.

5. **Portability** - you need the option to “de-tokenize” if you sell a business unit or change payment processors. Make sure your provider can obtain a mapping file from the incumbent and then produce a file for you with new tokens mapped to your old token values.

6. **Ease of Implementation** - tokenization shouldn’t require a substantial coding effort. Look for clear, well-written documentation, a robust test and certification system, and dedicated implementation personnel.

7. **Unlimited Use** - the most cost-effective tokenization solutions charge you only when you create a new token and the provider places the PAN in their “vault.” As long as the card number doesn’t change, you shouldn’t have to pay for recurring charges, storage fees, or per-transaction fees.

8. **Ease of Compliance** - when you conduct a yearly assessment of your company’s PCI DSS compliance, the primary method for discovering vulnerabilities is to see if your “data footprint” includes PANs. All the major card brands use values that pass what are known as “Mod 10 validations” or “Luhn checks.” If the tokens you store also pass the Mod 10 check, it can be difficult to prove that you aren’t storing PANs. The best format for your tokens is to be “Mod 10+1” checked, which means scanning software won’t falsely identify your tokens as PANs. Also, Mod 10+1 tokens will never be mistaken for a credit or debit card and will be completely useless if stolen.

**Tokenization Workflow**

![Tokenization Workflow Diagram]
Address verification service (AVS)

Address verification service (AVS) is an automated fraud prevention service designed to reduce the risk associated with online transactions. It helps minimize fraudulent transactions by verifying the cardholder’s billing address with the card issuer. Your business must initiate the AVS check by providing the proper data in each transaction. Verification results can help you decide whether to accept a particular order or take follow-up action.

AVS uses two pieces of extra information in the authorization request you send to your payment processor: the numeric portion of the cardholder’s address and the ZIP code. For AVS to work, your payment processor forwards this information to the holder’s issuing bank, who then issues an AVS Response Code that merchants can choose to evaluate in determining whether or not to accept a payment.

How to use AVS

AVS is transparent to your customer and applies to payments using Visa, MasterCard, American Express, and Discover cards.

To best leverage AVS responses, your business should:

- Ask the customer for the billing address and ZIP as it appears on their monthly statement.
- Submit the billing address and ZIP fields as provided by the customer with the authorization request.
- Understand all AVS partial matches. A “partial match” indicates that the billing address being compared has the same ZIP code or the same numeric values in the street address, but not both. A “no match” response indicates that neither part of the billing address matches your data.
- Understand AVS “no match” responses carefully, as they are typically a useful indicator of potential fraud. However, because not all AVS “no match” responses necessarily indicate fraud, a “no match” signal should prompt further steps to authenticate the order.

→ TIP: A “no match” response does not automatically result in the authorization being declined. Understand how your processor treats these “no match” responses as you may be able to have them auto-decline OR avoid them from declining to improve your approval rates.

Why is AVS important?

A positive AVS response is one way to remedy many “Unauthorized Use” and “Non-Receipt of Merchandise” chargebacks. Without a positive AVS response, online merchants have no dispute rights for some card brands. Also, Visa transactions using AVS are given a better interchange rate than those that do not, even if the AVS fails.

However, AVS is not foolproof and should be combined with other internal and external fraud detection tools.
Card security checks

To help reduce fraud in online commerce, the major card brands implemented authentication systems to determine if the credit card used in a transaction is in the possession of the owner. Knowledge of the card security value — known as CVV2, CVC2 (Card Verification Value/Code), CMID (Card Member ID), and CID (Card Identification Number) by Visa, MasterCard, Discover, and American Express respectively — proves that the purchaser has seen the card, or has seen a record made by somebody who saw the card.

What are CVV2, CVC2, CMID, and CID?

The image below shows the location and number of digits used by each major card brand. Visa, MasterCard, and Discover use a three digit code in the signature strip, while American Express uses a four digit code on the front of the card. When collected, submitted, and substantiated during the authorization process, the security value significantly increases the probability that the person placing the order is in possession of the card. In combination with an AVS check, the card security value is a useful tool to help minimize fraud from stolen card numbers and counterfeit cards.

How CVV2, CVC2, CMID, and CID work

• The card security code is requested from the customer and sent to the processor as part of the authorization request.

• The processor — working through the card brands — submits the code to the card issuer to determine its validity and then sends a Response Code back to your business along with the authorization.

• The merchant evaluates the Response Code, taking into account the authorization decision and any other relevant or questionable data, like the AVS response.
Why are CVV2, CVC2, CMID, and CID important?

Better fraud protection

CVV2, CVC2, CMID, and CID can help merchants differentiate between good customers and criminals. For example, these security codes can prevent most fraud from cards obtained via “trash diving” or “skimming” techniques. CVV2, CVC2, CMID, and CID enable the merchant to make a more informed decision before completing an online sale.

Reduced chargebacks

Using card security checks potentially reduces fraud-related chargeback volume. While it doesn’t eliminate the risk of fraud, this additional security feature is designed to protect your business by verifying that the card is present during the purchase.

Fraud filters and fraud scoring

Perhaps the easiest way to avoid the downstream costs of fraudulent transactions is to stop them from happening in the first place. This is where security solutions like fraud filters and fraud scoring can help protect your business. By identifying anomalies in transactions before they’re approved, your business can avoid the hassles and costs associated with manual review, chargebacks, and reputational damage that often accompany fraud.

The following fraud filters may be available for your online payments program:

- **Address verification service (AVS)** – automatically filters transactions based on the AVS ZIP or street match responses from the card brand
- **Card security codes** – automatically filters transactions that don’t match the CVV2/CVC2/CMID/CID value that the issuing bank has on file for the card
- **Card velocity** – automatically filters transactions once a threshold number of approved authorizations/sales occur within a preset time period
- **Prior chargeback** – automatically filters transactions based either upon the receipt of any chargeback by the merchant from the same account within the last 200 days, or only the subset of chargebacks with fraud-related chargeback codes
- **Prior fraud advice** – automatically filters Visa and MasterCard transactions if the merchant has received a prior fraud alert from that specific account
- **International card** – automatically filters Visa and MasterCard transactions originating with cards issued in either all foreign countries (i.e., non-U.S. issuers) or specific foreign countries designated by the merchant
- **Prepaid** – adjustable filters for prepaid cards and can also be configured to detect non-reloadable prepaid cards
Some of the more advanced fraud scoring solutions use network intelligence to scrutinize transactions and flag possible fraud on parameters, including the following:

- **Device fingerprinting** — device attributes are gathered from every user interaction to detect possible fraud; tracks the unique fingerprint and reputation of each device it encounters

- **IP proxy detection and piercing** — exposes the true IP address of every transaction to expose fraudsters that may be trying to conceal their true identity

- **IP geolocation** — IP geolocation combines with IP proxy piercing to identify the customer’s true location

Work with your payments partner to identify which fraud filters and fraud scoring solutions might be a good fit for your online business.

>> **TIP:** While many fraud filter types and combinations of them are possible, fully understanding your organization’s fraud footprint will be critical in determining which settings will be the most effective. Consult with your processor for assistance in determining your best options.
Conclusion

When conducting business online, there are many options to consider when it comes to fighting fraud and improving data security. From understanding different types of online fraud to the critical role of PCI DSS compliance, through to data security solutions that are appropriate for your business, it can be an overwhelming process.

This is where an experienced, trusted payments partner can help guide your journey toward safely and securely accepting payments online. Select a partner that’s aware of the different types of fraud that exist in online commerce and that can quickly adapt to the ever-changing techniques of sophisticated criminals.

Also, make sure your payments partner is highly knowledgeable in helping online merchants comply with PCI DSS. An experienced processor can offer you comprehensive support on meeting and maintaining PCI DSS compliance through system vulnerability checks, training programs, and customer support. Finally, make sure they offer advanced data security solutions like tokenization, AVS, card security checks, and fraud filters/scoring to build the best offense for your online business.

When you work with a reputable payments processor that prioritizes security, you can breathe easier knowing that your business and your customers’ data are both secure.