First Data

A First Data White Paper

October 2010

Strategies for Reducing the Risk of eCommerce Fraud

Fraud techniques are constantly evolving, and new data breaches are reported every day—are your online security practices adapting rapidly enough?

By:
Theresa Ward
First Data

Introduction: The Realities of eCommerce Fraud

In spite of a weak economy, one business segment—eCommerce—has continued to experience significant growth. In 2009, eCommerce sales grew by 5.5 percent, to $205 billion. According to Javelin Strategy & Research, online retail sales are expected to increase by another 13 percent in 2010.[1]

Although eCommerce fraud rates have stabilized in recent years—due, in part, to retailers' increased vigilance—in 2009 merchants still lost $3.3 billion to online fraud.[2]

The sustained growth of eCommerce continues to attract criminals who continuously develop new schemes to defraud merchants and their customers. These cyberthieves persist in devising increasingly sophisticated ways to steal personal account information from merchants, and to accumulate goods, services, and quasi-cash through unauthorized use of that information at merchant Web sites.

Some smaller merchants respond to the threat through stringent, manual review of online purchase attempts. This can be costly, and it distracts staff from revenue-generating aspects of operating the business. Yet businesses do need to aggressively manage fraud if they intend to avoid being victimized by cybercriminals.

Two Common Fraud Misconceptions

The liability to merchants for eCommerce fraud is the same as for fraud perpetrated in brick-and-mortar stores.

FALSE: Merchants are more likely to absorb the losses in fraudulent eCommerce activities.

Merchants need to develop their own sophisticated security expertise to protect against ecommerce fraud.

FALSE: Outsourced services available to merchants have powerful fraud prevention features built into them.

This paper takes a closer look at the two facets of fraud management that are of primary importance to online retailers of all sizes:

- → Protecting against the theft of customer data
- → Preventing unauthorized use of consumer data in fraudulent transactions

In both cases, there are tools and services available for even the smallest merchants to reduce the costs of defending against these threats—enabling retailers to pursue eCommerce revenue opportunities without assuming excessive fraud risks or employing time-consuming manual practices.

Protecting Customers' Confidential Information

Any business that stores personal data, such as customers' payment card information, is responsible for keeping that information secure. This is true of online businesses as well as brick-and-mortar organizations.

Why should the security of personal data be important to a retailer? When a data breach occurs, it requires remedies that are costly to the breached organization. These costs can be enormous. According to a study by the Ponemon Institute, resolving data breach incidents cost U.S. companies $204 per compromised record in 2009. Of the 45 data breach cases studied, the least expensive total cost of an incident was $750,000.[3]

Even worse, the total eventual damage to an online business can be even greater. Data breaches produce unwelcome publicity that can have a severe negative impact on a retail organization's brand and reputation. The damage from a data breach often extends well beyond losing the trust of only those customers directly impacted by the incident—and negative public perceptions can persist for years after a breach.

One of an eCommerce business's primary responsibilities related to data security and fraud management is the requirement to comply with the Payment Card Industry Data Security Standard (PCI-DSS), which is a set of obligations mandated by card networks to help protect consumers' personal information.

These PCI requirements pertain to how the data is stored, accessed, and handled by a business. Organizations that store account information are required to certify that they are in compliance with PCI standards. This certification process, which must be done periodically, can be expensive and time-consuming.

Large numbers of small- and medium-sized merchants are somewhat bewildered by PCI compliance, according to a July 2009 survey conducted by ControlScan, the National Retail Federation and the PCI Knowledge Base. "The standard is meant to keep their customers' data safer but understanding it has proven difficult for small merchants," asserts the group's research report.[4]

Fortunately, there are services and solutions available to help eCommerce merchants both avoid data breaches and achieve cost-effective PCI compliance. These services assess the overall cardholder data environment, recommend ways to minimize compliance costs, protect transmitted data, and conduct annual audits to maintain compliance. In addition, service providers can help merchants implement innovative new approaches to data security, such as tokenization and end-to-end encryption (see First Data's white paper, A Primer on Payment Security Technologies: Encryption and Tokenization, for more information on this topic).

Data security and PCI compliance services are often available from payment processors, and these services can be well worth the investment. Large payment processing companies handle enormous amounts of personal data, and they must maintain the highest standards of compliance to stay in business. Outsourcing data security to organizations equipped to manage it can reduce the cost and burden of maintaining PCI compliance certification.

Do merchants have to become fraud experts?

It's easy to see why many executives of small to mid-sized e-merchants are buffled by fraud and security management matters

Running an eCommerce business during a difficult economy demands the bulk of management's time. They have little time left over to understand ever-changing fraud trends and prevention techniques.

eCommerce executives should not have to become experts in the many aspects of fraud management, nor should they need to hire staff specifically dedicated to fraud expertise. The field is too complex, and most small business leaders should be focusing on marketing, finance and operational matters, not the constant attention fraud management requires.

By relying on service providers, executives gain expertise and technology to accurately and efficiently address the key issues of fraud management, such as:

- What are the emerging fraud trends in eCommerce?
- What are the major "red flags" of fraud for different types of orders?
- How can all orders be efficiently screened for fraud risks, with a minimum of costly manual reviews?
- What is the best way to prevent the interception of transaction data?

PCI-DSS compliance is one important step toward maintaining secure eCommerce operations. According to a recent study, retailers that experienced a data breach were 50 percent less likely to be PCI compliant than the overall merchant population.[5] However, it is important to note that PCI-DSS is narrowly focused on keeping stored data from being hacked or compromised. Complying with PCI-DSS does not prevent identity thieves from using data already compromised from another source. While providing a more secure transaction environment and helping to reduce the overall quantity of stolen card data in circulation, compliance with PCI-DSS does not protect the merchant from accepting potentially fraudulent transactions at checkout.

Online Orders Pose Unique Challenges to Merchants

eCommerce businesses sometimes erroneously assume that their merchant account provider is financially liable for fraud and disputed transactions. They also don't realize that according to industry regulations, card-not-present (CNP) merchants are responsible for confirming shoppers' identities and dealing with disputes associated with unauthorized purchases. Many online retailers rely only on address verification, card code verification and the card network's authorization to evaluate the legitimacy of purchase attempts. It is imperative that merchants realize that payment fraud is evolving every day, and relying on just one or two factors related to an eCommerce purchase is not a dependable way to identify and stop unauthorized card use.

When payment fraud occurs at checkout, the merchant incurs the greatest losses—not the victimized consumer or the card issuer. According to a study by Lexis-Nexis Risk Solutions, merchants lose 10 times more than banks, and 20 times more than consumers, due to fraud each year.[6]

With online and other CNP transactions, there are no signed receipts to protect even merchants that follow the validation rules of the card networks. There is also no ability to examine identification cards and match signatures; nor is there physical evidence of the customer making the purchase. None of the protective mechanisms present in a physical store are available in the eCommerce world.

Even a small percentage of disputed purchases or fraudulent chargebacks can significantly erode an eCommerce merchant's profit margins. Chargebacks are the final result of the dispute process in which a cardholder challenges the legitimacy of a purchase made on his or her payment card. Chargebacks can occur up to six months after the transaction, and must be reimbursed by the merchant that processed the order. Chargebacks, however, are just one component of fraud losses. Other costs include the replacement cost of lost goods, shipping expenses of goods sent to a non-paying shopper, chargeback dispute fees, and possible legal and administrative costs associated with reviewing transactions and resolving disputes.

Excessive chargebacks can also lead to an even more problematic issue: failure to meet association fraud rate standards. If chargebacks exceed just 1 percent in a particular month, a merchant may be placed on a "watch list"—the networks' version of probation. If losses are not reduced within 90 days, the merchant may lose its ability to accept credit card payments altogether.

Tools for Detecting and Preventing Fraud Transactions

Because of the risk inherent in a CNP transaction environment, many merchants have attempted to develop comprehensive strategies for detecting and preventing fraud. With the right tools and technologies, merchants can apply these strategies to safely conduct business online without simply accepting fraud as a "cost of doing business."

Until recently, many of the best risk assessment and fraud management solutions were designed and targeted only towards larger merchants—even though merchants of all sizes are equally vulnerable. In fact, merchants with smaller sales volumes can be at even greater risk due to relative inexperience in fraud detection and a lack of dedicated fraud management resources. Fortunately, powerful tools and technologies for fraud management are now available—and affordable—for merchants of all sizes.

With these technologies, eCommerce merchants have the opportunity to implement fraud management programs using any or all of these three key functions:

1. Automated transactional risk scoring

Specific logic and settings can help to distinguish normal purchase behavior from risky transactions. Fraud risk is calculated based on multiple data factors and assigned a numerical score for each transaction. The scores, which serve as relative risk indicators, determine "next steps" for that transaction according to a merchant's preferred operating procedures.

2. Real-time categorizing and resolution

Transactions with risk scores exceeding certain thresholds—determined by either the merchant or the fraud solution provider—can be automatically placed into different categories for further action. Generally, a transaction is either immediately accepted or rejected—but it can also be flagged for manual review if it falls somewhere between those two categories.

Depending on the fraud solution provider, this categorization process may require manual efforts to synchronize with the authorization, settlement, and fulfillment procedures. Fortunately, some providers allow the fraud service to operate "in-line" with the payment authorization flow, requiring minimal intervention by the merchant, and streamlining business processes.

3. Post-purchase transaction management

Optimal fraud service offerings should also include an interface for reviewing transactions that fall between the "accept" and "reject" thresholds, so that members of the merchant's staff can determine the appropriate activity on a transaction with a single dashboard. The dashboard can include multiple tools and features to assist merchants not only with the initial resolution of a transaction, but follow-up activities such as reporting and performance analysis.

It is important to note that the life cycle of fraud management does not begin and end simply with the purchase attempt. In order to continue proactively handling fraud attempts (as well as to resolve chargebacks and disputes efficiently), merchants need a database that can maintain detailed records and be used to understand transaction trending over an extended period of time.

Re-presenting and resolving fraudulent chargebacks can be a complex and time-consuming effort. Dashboards like the ones mentioned above can help easily extract details about a transaction to help win re-presentment attempts. Some fraud solution providers will outsource transaction review and chargeback re-presentment efforts for an extra cost. Merchants need to evaluate the appropriate level of risk management they can administer internally versus outsource, dependent on budget, staff, and other resources available.

4. Adjusting Fraud Rules and Parameters

One common pitfall to avoid is the "one and done" mentality—too often, merchants dedicate a resource to configuring fraud parameters once, but not to ensuring that the parameters are still relevant weeks, months, or years later. Fraud trends evolve rapidly and detection tools need an equally quick response to remain effective. Regardless of which tools merchants are using to prevent fraud, those tools should be referenced against reports and analytics on a regular basis. Merchant staff should also be trained to react to immediate critical occurrences, such as a sudden attack from a fraud ring in a particular geographical location. These may require significant—but temporary—changes to the existing fraud settings.

With these powerful fraud management capabilities, online retailers of all sizes can efficiently:

- → determine what levels of risk are acceptable for various products, order profiles, shopping behaviors, and other combinations of factors
- → adjust rules and logic as needed, based on evolving fraud patterns
- → easily categorize all orders, ideally including a resolution procedure that flows "in-line" with the payment process
- → streamline administrative processes during the entire life cycle of a transaction

By integrating fraud management tools into checkout processes, even small eCommerce businesses are empowered. Fraud management becomes an intuitive, practical, controllable business process.

How Does Risk Scoring Work?

Online retailers can use dozens—or even hundreds—of different factors to screen and categorize all attempted purchases for indicators of possible fraud. These data factors can be focused on payment method details, shipping choices, velocity (or frequency) behavior, geo-location details, and other characteristics. The more data that is collected and referenced to determine each transaction's score, the more accurate that score will be.

The more advanced risk assessment models typically use a scoring engine to compare as many transaction characteristics as possible against fraud triggers defined by the merchant and the service provider. Here are some examples of rules that might contribute to a negative risk assessment:

- → A single IP address has been used with multiple payment cards in the last "x" days.
- → The shopper's billing address is more than "y" miles from the shipping address.
- → The e-mail address has been flagged in a negative database of known fraud activity by other merchants participating in the same fraud detection strategy.
- → The BIN (Bank Identification Number) on the payment card indicates the transaction comes from a high-risk country.

Using a combination of these factors can be especially beneficial for merchants engaging in international eCommerce, where factors like address verification are unreliable by themselves.

An algorithm calculates a numerical score based on a weighted point system assigned to each "rule" like those listed above. For example, if the first rule (IP address) is triggered, it may add 50 points to the score. And if the third rule (e-mail address in a negative database) is triggered, it may add another 250 points to the score. Each score is then matched against a merchant's profile settings to determine how the transaction is to be resolved or reviewed. Risk scoring parameters enable near-instantaneous analytical and workflow results.

Online retailers should select a fraud solution provider that allows simple and frequent adjustments to scoring parameters, based on a merchant's preferences and ability to review transactions manually.

Different businesses can set up widely varying scoring parameters and order resolution rules to address their specific needs. For example:

- → A seller may deem requests for overnight delivery of heavy items or high-quantity items to be an order that requires review, while overnight delivery of one small camera is considered completely normal.
- → Items that are considered staples or commodity products may have less rigid rules than luxury items, such as electronics and jewelry, which are more likely to appeal to fraudsters.
- → An airline could set up stricter fraud policies for holiday flights or international destinations.

Risk assessment reports help analyze the effectiveness of manual reviews, and spot opportunities to eliminate costly review practices when analysis shows them to be unnecessary. According to one study, merchants ultimately accept over 70 percent of the orders they manually review, and 57 percent of merchants accept 90 percent or more of manually reviewed orders.[7] To cut review costs, merchants may prefer to limit manual reviews to suspicious transactions exceeding certain dollar thresholds, which can vary by product, geography, or other parameters.

With these sophisticated yet user-friendly capabilities, merchants of all sizes can significantly bolster their defenses against the high costs of fraudulent transactions.

Address Verification Systems

Address verification systems (AVS) are a widely- used fraud detection tool, but one that is no longer effective on its own for several reasons. For example, AVS does not apply to international purchases. In addition, legitimate customers may mistype their address or use a new address not yet known to their bank. On the other side, fraudsters often know to make sure the billing address and the billing zip code match in order to get an AVS match response. AVS should always be used for the best interchange qualification and for additional safety, but is only one of many factors used in overall risk calculation.

The following illustration shows how the scoring and assessment process can work in real time as a transaction is being processed.

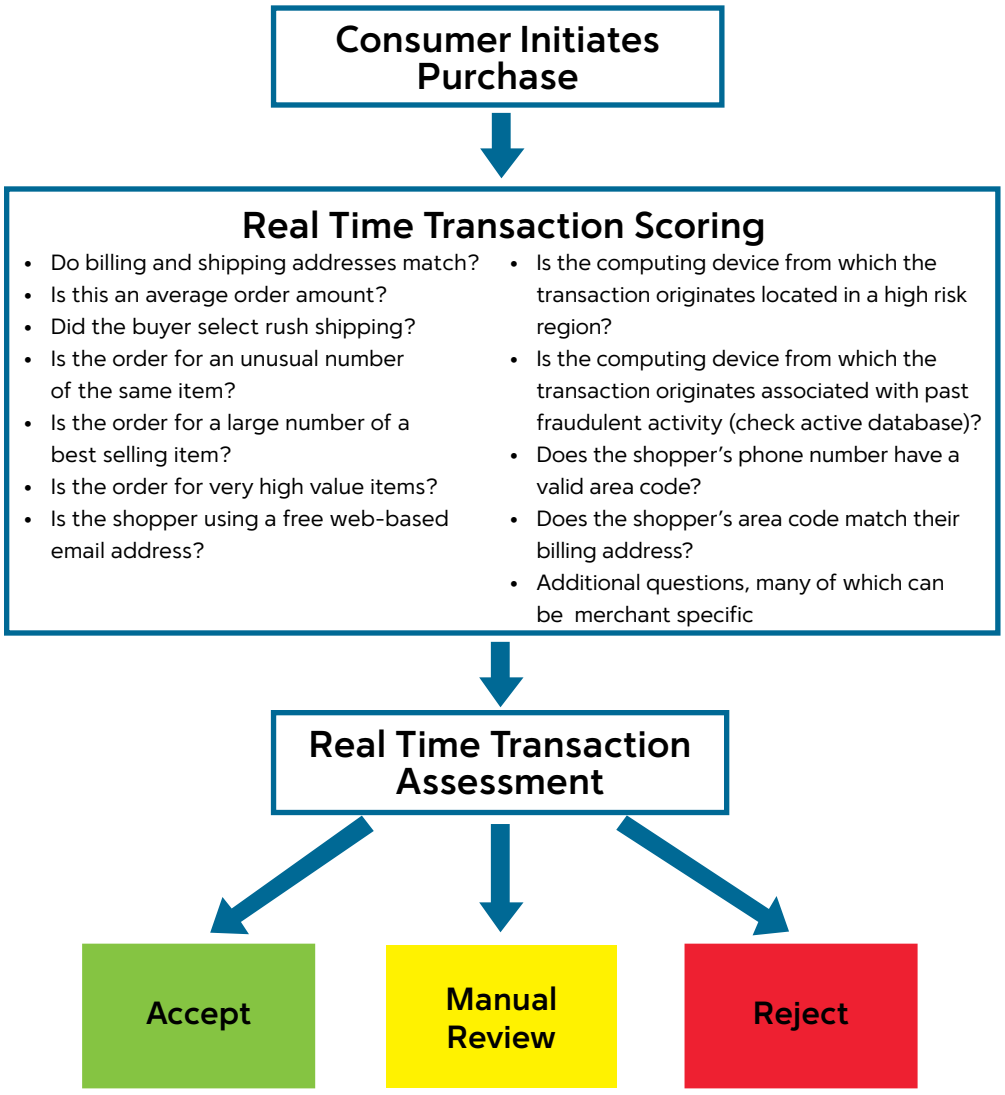

Figure 1. *This is a simplified illustration of how a transaction scoring and assessment process can become an automated part of processing any on-line transaction. Note that in a real instance there may be hundreds of questions and factors that go into evaluating the risk of a transaction. Also, a good automated risk assessment system should provide merchants with flexibility around the actions they can take based on scoring.*

Integrating Risk Assessment with the Payment Process

It is important to note that fraud management is more than just scoring, flagging, and reviewing transactions without regard to the other components of the purchase process. An order's score and resolution should directly drive authorization, settlement, and fulfillment activities. For example, fraud services built into payment processing platforms can reverse a transaction's authorization and release the funds-hold on the buyer's credit card if the risk score subsequently prescribes a "reject" action. Parameters can also be set to ensure that while a real-time authorization response may be given to a shopper during checkout, settlement cannot occur on a transaction that is pending further review by the merchant staff—or that orders in the

pending review queue for too long are automatically processed to avoid the expiration of an authorization. This gives the merchant complete resolution of each transaction with minimal manual involvement.

By making scoring-based transaction fraud detection an integral part of the entire payment processing function, merchants are capable of assessing the risk of transactions faster and more accurately, and are able to do this with much less investment of their staff time. Overall, they can focus on appealing to new customers, and rewarding their "good" customers, while eliminating time spent on the "bad."

Keeping up with the Latest Threats

Cybercriminals don't stand still—and neither should the security measures of online retailers. That is why successfully managing eCommerce Web site fraud needs to be an ongoing process, not a one-time fix.

Payment processors and other service providers can help new and growing merchants keep up with the constantly changing security landscape. They typically observe fraud trends closely and update their services promptly to protect against emerging fraud methods and techniques.

For example, some of the more sophisticated fraud management tools now employ device fingerprinting, which tracks specific details of the computer or smart phone a shopper is using to place orders. By checking to see if the buyer's device has ever been associated with fraud (along with other device-specific risk factors), this new technology has exciting potential to curtail fraudulent purchases.

Shared databases of individual factors associated with fraud (e-mail, card number, IP address, and more) are another innovative opportunity merchants can take advantage of. Multiple merchants contributing millions of data points over time help fraud systems evolve and adapt across the board, and collectively help put us one step ahead of the fraudsters' game.

The Benefits of Fraud Management Tools for eCommerce Merchants

- Access fast, efficient ways to help filter out risks
- Instantly accept or deny most orders based on easily defined and easily changed rules
- Quickly adjust scoring and resolution parameters to optimize results for changing business needs
- Reduce staff time spent on costly manual reviews of orders that don't "fit the mold" of an ideal order
- Focus more staff attention on growing the business instead of thwarting fraud
- Stay current with the latest tactics of fraud perpetrators
- Reduce overall chargeback costs and use an integrated fraud dashboard to manage chargebacks that do occur

Summary: Make Security Management a Part of Everyday Business Operations

Whether a retailer's onlin e revenues are $50,000 or $500 million, protection from cybercrime needs constant attention.

Even without putting a fraud expert on the payroll, an eCommerce operation can take steps to effectively minimize the risks of transaction fraud at checkout. Advanced fraud management services are fast, flexible, and affordable. Even small online retailers can utilize sophisticated, real-time risk assessment as an integral part of the checkout process, and lay a foundation of security best practices on which their business can grow.

Online retailers should consider implementing these best practices:

- → Deploy a combination of end-to-end encryption and tokenization to simplify PCI compliance and protect customers' payment card data from being stolen and used fraudulently.
- → Make sure all employees understand the risks of card-not-present transactions. Compensate for the lack of in-store controls with real-time screening using both payment information and anti-fraud intelligence from other sources.

- → Enable proactive security measures. Don't accept fraud as "just another cost of doing business." Every eCommerce merchant can wield the power to detect and stop most attempts to make fraudulent online purchases. Configuring the right kind of fraud logic in the early stages of your business can help you avoid problems later.
- → Leverage as many tools as are available to you through your payment provider and other resources. Experiment with the use of automated order screening early on, when transaction volume is low and suspicious behavior anomalies are more easily recognized. Constantly re-evaluate the risk settings and resolution rules that will catch most fraud attempts without requiring many transactions to be reviewed or denied.
- → Participate in forums, webinars, and other shared experiences with fellow merchants; in many ways, collaboration is the greatest advantage we have against fraud.

Additionally, for support and guidance on the nuances of fraud management, eCommerce merchants should talk to their payments processor.

- → Ask how to use both payment and non-payment information to detect fraud and gain visibility into shopper behavior.
- → Get recommendations on how to define rules that effectively assess order risk and determine the appropriate resolution of each order.
- → Find out what level of support to expect in implementing industry best practices for reporting, scoring, order resolution and scoring parameters.
- → Find out if the payment processor's solution has a user-friendly workflow for resolving transactions and managing chargebacks and reversals.

For additional information about PCI compliance, data security, and automating fraud detection as part of a payment processing solution, contact First Data or visit our website at FirstData.com.

Sources

[1] Javelin Strategy & Research. "Online Retail Payments Forecast 2010-2014," February 2010

[2] The Green Sheet. "The Worldwide Fraud Web Exposed," April 22, 2010

[3] PGP Corporation and Ponemon Institute. "Ponemon Study Shows the Cost of a Data Breach Continue to Continues to Increase," January 5, 2010

[4] ControlScan, National Retail Federation, and PCI Knowledge Base. "What Small Merchants Know (and Don't Know) about PCI Compliance," August 2009

[5] Verizon Business. "Verizon 2010 Payment Card Industry Compliance Report," September 2010.

[6] LexisNexis Risk Solutions. "U.S. Retailers Face $191 Billion in Fraud Loses Each Year," November 9, 2009

[7] CyberSource. "Online Fraud Report, 11th annual edition," 2010

The Global Leader in Electronic Commerce

First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. Serving millions of merchant locations and thousands of card issuers, we have the expertise and insight to help you accelerate your business. Put our intelligence to work for you.

About the Author

Theresa Ward joined First Data in 2009 as product manager of First Data's Fraud FlexDetect solution, an integrated fraud detection and management tool offered within the First Data Global Gateway and Compass platforms. She is currently overseeing the development and launch of this product through a partnership with Accertify as the technology engine behind Fraud FlexDetect.

Before joining First Data, Theresa was responsible for managing partnerships with payment brand and payment authentication solutions at CardinalCommerce in Cleveland, Ohio. Other roles at CardinalCommerce included heading up the Advisory Council and selling payment brand and fraud protection solutions to top eCommerce retailers.

Theresa studied Organizational Communication at Bowling Green State University in Ohio.

For more information, contact your Sales Representative or visit firstdata.com.

301-1113-92110