First Data
b›yond the transaction℠

First Data Market Insight

Five Steps Towards Effective Fraud Management

Merchants doing business in a card-not-present environment are exposed to significantly higher fraud risk, costly chargebacks and the challenge of securing consumers' personally identifiable information (PII). Because it is much more difficult to validate a shopper's true identity in an online transaction, fraudsters often take advantage of eCommerce merchants to monetize credit card data that has been illegally obtained. They may use stolen card details to purchase desirable goods or access certain services. Fraudsters may also attempt small transactions or donations as a way to validate that stolen cards are 'good' before moving on to bigger ticket items. Addressed in this paper are five key steps that will help merchants design an effective fraud management strategy for their business.

STEP 1: First Things First ....

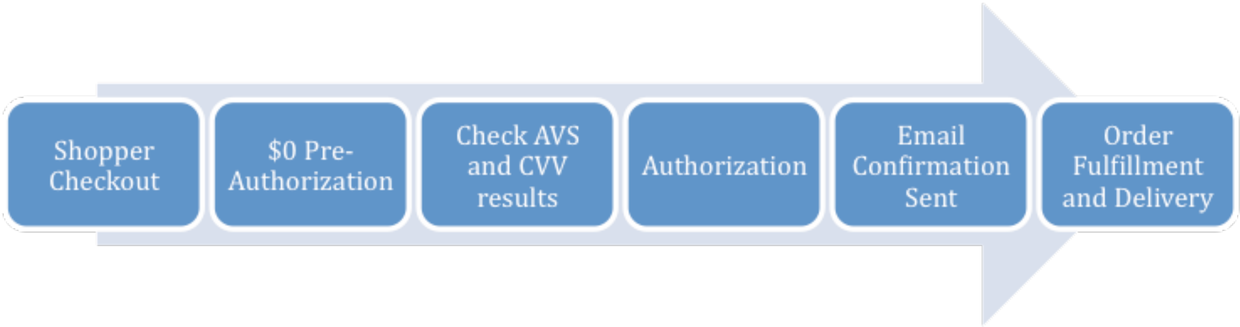
Before developing new strategies and processes, merchants should be sure to fully evaluate their existing business environment from several angles. Developing a new fraud strategy—or re-vamping an existing one—can only be effective once the following aspects are understood:

→ Who is your customer? What is their normal buying behavior? Do you manage multiple channels (call center vs. online, B2B v. B2C, etc.) where customers' purchase behavior may vary? It is extremely important to establish this foundation of 'normal' behavior so that you may uncover patterns that are indicative of fraud.

→ How and why are you currently subjected to fraud? Seek to uncover the source of existing or previous fraudulent claims and disputes. Are fraudulent transactions typically a lower dollar amount in frequent succession (a sign that fraudsters may be testing stolen cards)? Is it so-called friendly fraud, in which case the customer knew who used their payment details without permission? Are customers simply confused by your descriptor on their credit card statement? Is it related to shipping and receipt issues? Is there a certain payment or shipping method, country, or category of products that are associated with fraud attempts? By understanding these vulnerabilities you will know where to focus your efforts in a fraud strategy moving forward. The more specific you can get about your current challenges and future goals, the more effective your strategy can be—and the easier it will be to measure.

→ What fraud trends are common in your vertical? What type of fraud is impacting your competitors and peers in the industry? Uncovering such details may be easier said than done, but you may also find that your peers are willing to share their experiences and best practices as they are facing the same challenges in protecting their businesses.

→ Review your current authorization procedures to ensure proper use of issuer fraud tools. Do you perform pre-authorizations to check credit card numbers prior to fulfillment? Are you using $0 Account Verification transactions where applicable? Have you minimized use of $1 Authorizations which are subject to network (Visa) Misuse Fees? Do you have to void or reverse authorization messages when orders are determined to be fraud? Are you requiring Card Verification (3 or 4 digit code) be submitted on all transactions? Are you submitting billing address and zip code with the transaction to make use of issuer's Address Verification Service (AVS)? Are you issuing returns if a transaction is disputed? Understanding these core procedures may help uncover costs that can be eliminated with a new, improved fraud detection strategy. A representative eCommerce 'transaction life cycle' is below:



- → Review and prioritize all costs and consequences associated with online fraud before setting your fraud and security goals. While lost revenue and chargebacks might seem to be the obvious answer, a deeper dive can often uncover subtleties that are also impacting your bottom line. How is your brand or your reputation affected when a consumer's stolen card is used at your web site? Have you limited growth of your business (for example, not doing business outside the US) because of fraud and risk fears? Are your current fraud practices turning away good customers who will not return to your site in the future ("insult rate"). Do you incur unnecessary overhead costs associated with manual review of orders suspected to be fraudulent? Answering these questions can help set goals later on in the process.

- → Gather and document a full list of data elements that you collect from the consumer and use (or could use in the future) to identify fraud. Some examples include billing address, shipping address, IP address, email, phone number, AVS response and CVV response.

STEP 2: The Right Frame of Mind

Ensuring all relevant and impacted teams are on the same page is critical to any merchant's successful fraud strategy. Comprehensively discuss all tools and procedures that are used to maintain security and prevent fraud today. This includes everything from employee training to chargeback representment policies.

Also, investigate the tools that are available today that you may not be using. Tools may be available through your shopping cart, payment gateway, processor, or acquirer. If detailed explanations of these tools and services are not readily available, contact the support center or service representative who manages your account. Ask to review their latest offerings for detecting and managing fraud issues.

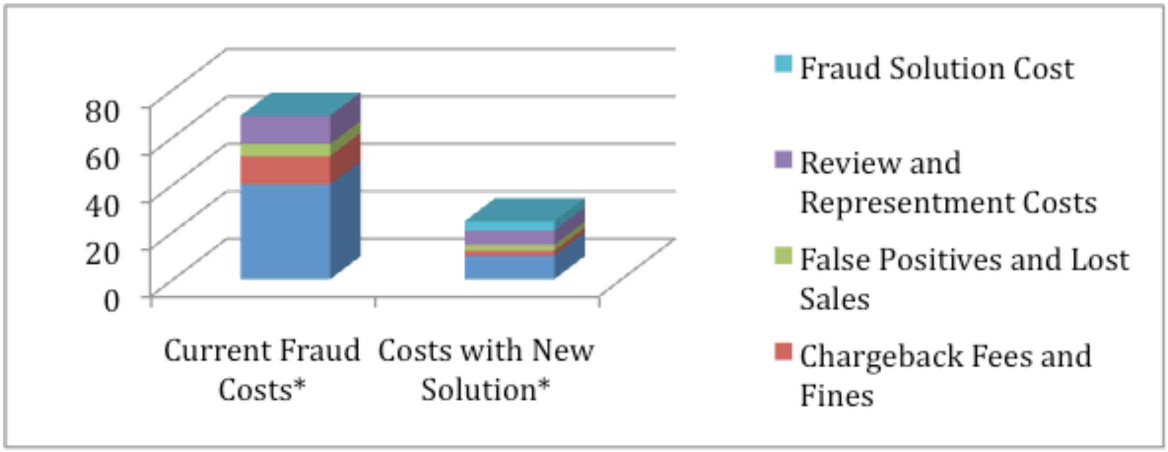
Before making any decisions about new solutions or services to use, your team should also be aware of relevant third-party offerings, to effectively compare what your existing providers may offer, what tools you can implement yourself, and what may be outsourced to a third party. Educate the team on available services and best practices by checking industry sources, for example:

http://www.merchantriskcouncil.org
http://usa.visa.com/merchants/risk_management/card_not_present.html

(This research and education should continue as an ongoing practice; and should be a part of your company's regular operations.)

Next, be sure that the stakeholders at your company are engaged—getting the team's buy-in to be proactive about fraud, and to do more than just the bare minimum, is critical to security and success. The data that you've gathered in Step 1 will help make this case.

Preparing a return on investment model may be helpful in analyzing the cost-benefit associated with changing your online fraud management strategy or implementing new services. Below is a simple example based on an eCommerce merchant**:



*In thousands of dollars annually

**Based on $5m eCommerce card volume annually

(More detailed ROI models available upon request).

STEP 3: The Human Element

In addition to getting your team on board with supporting improved fraud solutions, part of that team must be dedicated to (and accountable for) overseeing the execution and management of your eCommerce fraud strategy. This individual or team could take leadership on a range of responsibilities including:

- Setting goals—immediate and long term. This may include keeping fees below a certain dollar amount, keeping customer complaints below a certain volume, or improving review productivity by a certain percentage. Success can be achieved by the entire company, but should be driven by one department.
- Choosing ways to measure those goals and relative success—this team would be charged with creating/referencing reports and analysis where available.
- Research and awareness of new fraud trends developing inside and outside the company
- Proactive interaction with the appropriate providers and channels for support and issue resolution (especially when new fraud trends are noticed)
- Maintain positive and negative lists of customer data—to be further addressed in Step 4
- Work with IT when changes are needed and cannot be addressed by the existing system
- Communicate to employees company-wide, on what to look for that may indicate new risk patterns
- Communicate to employees company-wide, on fraud and risk policy details that should and should not be shared with customers
- Determine when and how to work chargeback re-presentment in an effort to recover funds
- Keep the company on track for a long term fraud strategy—remember chargebacks can occur up to six months after the transaction took place, so true goals may only be measured over time.

STEP 4: Pick Your Tools ...

Merchants who have experienced fraud in the past have become aware of a critical lesson: Fraudsters evolve. And quickly! Because they rapidly adapt their strategies, any tools put in place by the merchant must be comprehensive and cutting-edge in order to stay one step ahead. Utilizing only one or two points of logic (i.e., rejecting orders simply based on dollar threshold or AVS results) will rarely identify fraud attempts accurately, causing overabundant review efforts and potential "false positives" (turning away good sales, resulting in a high customer insult rate). Unfortunately some detection tools (like AVS and CVV checks) have lost some effectiveness as they have become more mainstream. Risk detection must be based on all available elements of purchase behavior. This is why, in Step 1, we suggest you document a list of the elements that you can capture about your consumer's interaction with your store. The more data you have, the more accurately you can detect and prevent fraud. Below are several tools you can use to process the data elements and effectively take action on fraud attempts.

→ A **scoring engine** (available through a third party or something that some merchants have built in-house) is one of the best tools to calculate risk based on multiple data elements collected on a transaction or over time. A scoring engine should reference **distance calculations, velocity, device reputation**, and more. A scoring engine should be weighted and flexible, to specifically adapt to your business model. Scoring should also occur in real time, rather than evaluating the frequency of a data element seen once or twice daily, and the rules should be flexible to rapid changes.

→ Scoring engines usually generate a numerical value, but this number is arbitrary unless you understand the score ranges and activity set to each of those ranges. Activities triggered by the numerical score will allow you as a merchant to take action against fraud, instead of just being able to view it. This part of the fraud management process is called a **decisioning engine** and is optimal when leveraging a manual review process, rather than using blocking or negative lists alone.

→ Examples of **negative lists** are credit card numbers, shipping addresses, or other elements that have previously been associated with fraud and therefore are no longer acceptable by the merchant. Rejecting orders based on lists—although helpful in many cases—should never be considered permanent, as "good" credit card accounts can be compromised and "bad" elements like phone numbers may be reassigned.

→ Participating in a **shared database** can improve fraud visibility and awareness as well. In addition to your own comprehensive details and history about a customer, shared database tools provide insight into what your fellow merchant community has identified as fraud. Participate in reputable shared databases whenever possible, if cost effective.

→ Services that eliminate or reduce merchant liability for fraud can be an effective addition to, but not replacement for, fraud scoring and screening tools. The most widely accepted solution globally is **3-D Secure**, also known as **Verified by Visa and MasterCard SecureCode.** These authentication protocols, when implemented correctly, can reduce chargeback volume significantly and also help merchants qualify for lower interchange rates. When evaluating the integration and use of the 3-D Secure technology, it is important to work with a reputable provider to understand the IT effort and cost that may be involved, as well as best practices to avoid negatively impacting the shopper experience.

→ Lastly—all the data, services, settings, results, and activities are only effective when housed and displayed in a user-friendly **review interface** that meets your company's needs for reporting, analysis, and other measurables towards your goals. Ask your current providers what reporting and fraud setting wizards are available and attempt to leverage a comprehensive, pre-built, yet customizable solution rather than building one yourself, if cost effective.

Step 5: Key Takeaways

Fraudsters aren't going to "quit"—they're only going to get better, and smarter. Although there is no silver bullet to ensure that your business is protected from fraud attempts 100 percent of the time, you have many options at your disposal to stay one step ahead of them. Your team can use partnerships, tools, and resources to strike a balance on an effective fraud strategy, and continue to evolve through this constantly changing environment. Proactive decisions you begin to make today can help prevent chargebacks, fines, customer complaints, and merchant account damage overall in the future.

In addition to the steps we've outlined in this paper, we recommend that you keep these three ideas in mind as you build your fraud strategy:

1. When you develop your strategy and measure your results, make sure it considers the full, end-to-end lifecycle of a transaction.

2. Don't copy and paste your fraud strategy from someone else—make sure it uniquely applies to your consumers and your business, and can change as your business grows.

3. Communicate your goals and procedures clearly to all relevant parties—EXCEPT the fraudsters. Don't share specific reasons with shoppers on why you reviewed or rejected an order, as fraudsters could be trying to uncover your tools and settings, so they can work around them.