Fraud Detection & Mitigation Strategies

Fraud is an inherent risk of accepting payments in eCommerce. Beyond costly manual review, lost goods, and expensive chargebacks, the impact of fraudulent payments can also tarnish your reputation. Fortifying yourself against all potential attacks with a one-time inoculation is impossible because fraudsters continuously adapt.

Acknowledging your potential exposure to these consequences is an essential first step. However, navigating the burgeoning wealth of industry knowledge can be overwhelming. Start by understanding three key aspects of successful mitigation strategies and how you can apply them to common types of attacks.
Three Building Blocks of Fraud Detection

Fundamental building blocks of an effective mitigation strategy include authentication, deviation, and reputation. Keep in mind that these building blocks are complementary. The most effective fraud mitigation strategies combine all three to achieve greater precision and efficacy than the sum of its parts. Assemble your own mitigation strategy with these building blocks to help minimize your fraud exposure and reduce the impact of false-positives on your good customers.

AUTHENTICATION

Authentication asks a buyer to provide information to prove they are who they say they are. Consider your last call to your credit card issuer. Having an account number or address typically isn’t enough to prove you are the account holder. Additional information such as a PIN number or the last 4 digits of your social security number is typically required before you’re allowed to manage your account. Two common examples in payments acceptance include verifying the cardholder’s billing address on file and card security code (i.e. CVV, CVC, and CID) physically imprinted on the card. Using additional data points to verify the rightful cardholder’s identity is essential to protecting your business and customers.

DEVIAION

Deviation allows you to detect fraud by identifying “typical” purchasing behavior for your customers and treating any deviation from that pattern with increased caution. For example, a customer purchasing 10 digital downloads over the course of an hour won’t raise any eyebrows. However, that same frequency might raise a red flag in the case of high-end electronic equipment or gift cards (a common purchase for those looking to launder money). This method—called a velocity check—is an example of deviation-based fraud detection. At the same time, fraudsters often adapt quickly by modifying their approach to conform to expected patterns. Therefore, a more inclusive, global, and cross-merchant picture is often the best way to expose the anomalous buying behavior of clever fraudsters. That’s why participating in and leveraging the shared intelligence of a network of pooled payment, device, and identity data is so important.

REPUTATION

Incorporating reputation into payments acceptance is another way to inform an effective fraud strategy. This might be something as simple as a blacklist of bad customers—the modern equivalent of a sign above the cash register that says, “Do Not Accept Checks from These People!” Rigorously reviewing payments from devices with a history of fraud is an advanced application of this building block. Anyone who has applied for a loan knows the importance of reputation, which in this scenario exists in the form of credit history. As with a credit check, the power of shared insights plays an essential role in identifying reputation as fraudsters often attack multiple merchants. Each incident of confirmed fraud by another merchant can help you avoid the same fate. Reputation also helps you retain good customers by balancing the occasional anomaly against a history of good-faith purchases.

1 https://www.frbatlanta.org/documents/rprf/rprf_pub130117_wp.pdf
Common Fraud Attacks and Mitigation

Of the three most common fraud attacks is one found across industries, simple card theft. Two others, card testing and package interception/redirection, tend to target specific verticals.

**ATTACK #1
SIMPLE CARD THEFT**

Fraudsters employ several methods to obtain payment card numbers. What they do next separates the amateurs from the more advanced perpetrators. Less sophisticated fraudsters often pursue quick hits by purchasing products online—both hard goods and digital—with no intention of ever paying. Fortunately, many of their attempts can be foiled effectively with a no-frills fraud detection strategy.

**How can you mitigate simple card theft?**

**Authentication**

Enacting billing address verification (AVS) and card security code validation (CVV, CVC, and CID) is a must. While persistent fraudsters often find a way to overcome this gate, many do not. These forms of authentication are not cure-alls, but they do serve as relatively simple, low-effort tripwires to thwart less resourceful fraudsters.

**Deviation**

Once a fraudster identifies a working stolen card, it’s only a matter of time until the card is flagged for suspicious activity. As a result, they often buy products in ways different than typical consumers and you can use these deviations to your advantage. Employ a velocity check by limiting the frequency of payments from a given card to conform to typical patterns. Also, flag any orders with quantities or transaction values beyond the norm. These atypical behaviors may indicate a fraudster rushing to buy as many stolen goods as possible before his window of opportunity closes.

**Reputation**

Less careful fraudsters may leave a trail that you can exploit. Many merchants employ the use of a blacklist to shut out prior offenders. Track payment card numbers, IP addresses, email addresses, and other indicators of those who have a history of committing fraud. When scaled to an intelligent global network, this approach can provide a more effective defense.
**ATTACK #2  
CARD TESTING**

After obtaining a bulk of stolen card information, fraudsters must distinguish those already reported to issuers. Fraudsters solve this problem by “testing” each card with an online payment submission. Approved? It’s show time. Declined? Not so much. Merchants marketing lower-priced digital goods (e.g., non-profits accepting donations and online service providers like web hosting and domain name providers) are common targets. The key to successful testing is to stay under the radar, as legitimate cardholders are more likely to overlook lower charges—especially if they’re associated with a charity they recognize.

Testers can sell these good cards to other fraudsters at a premium further down the stolen card supply chain. Merchants, on the other hand, are left with high chargeback counts and the associated labor expense involved in manual review and response. These attacks rarely make headlines as fraudsters typically aren’t discovered until later, if at all. For example, Irish charity Jack & Jill received the equivalent of $180K in fraudulent donations online over a six week period last year as a result of card testing attacks\(^2\). These tangible losses, while substantial unto themselves, are compounded by the intangible reputational damage that might make existing and prospective donors think twice.

---

**How can you mitigate card testing attacks?**

**Authentication**

Fraudsters look for card testing targets that offer the path of least resistance. Since they have to submit many payments, their job gets easier if there is less information required for each payment. That’s why authentication such as AVS and security code verification is essential, though for a slightly different reason than described earlier. Many fraudsters that can secure large sets of stolen cards can also procure the information they need to pass those authentication checks. However, that validation in and of itself slows down each payment and, thus, renders your site a less attractive target.

**Deviation**

As opposed to a typical buyer, card testers submit a high number of payments in short succession. Use this deviant behavior to your benefit. For instance, monitor device, IP address, and IP geolocation velocity to flag any anomalous purchase activity. If they use—even in part—the same device, web access point, or web proxy, you can catch them with precisely configured rules that trigger above a predefined threshold. Minimize friction for good customers and the number incorrectly turned away by tracking the number of unique accounts, payment cards, geolocations, or email addresses used on each unique device. While a good customer may submit an abnormal number of payments in a short time period, they’re not likely to recreate a new account or provide a new payment method every time.

Fraudsters, like the rest of us, look to technology to make their attacks easier. They often employ high speed, automated bots to perpetrate their card tests\(^3\). This presents another opportunity to detect their schemes. Unlike their carbon-based creators, bots exhibit unusual device characteristics and are capable of filling out and submitting checkout forms in milliseconds. Flag any orders that click “Submit” in less than half a second. While it may not catch more sophisticated testers, these building blocks do add up.

**Reputation**

It’s easy for card testers to change a payment card from one payment to the next. Fraudsters are adept at doing their dirty deeds before landing cards on blacklists. It’s not, however, as straightforward to cloak their device and true IP address. This is where reputational insight comes in handy. If you can uniquely identify each buyer’s device and/or true IP address (i.e. behind any web proxy), you can ferret out bad actors by looking at their history—especially if you can plug into a global intelligence network among industry peers to expand your footprint.

---


\(^3\) [http://www.computerworld.com/s/article/9228527/Cybercriminals_increasingly_use_online_banking_fraud_automation_techniques](http://www.computerworld.com/s/article/9228527/Cybercriminals_increasingly_use_online_banking_fraud_automation_techniques)
ATTACK #3
PACKAGE INTERCEPTION AND REDIRECTION

Card thieves will use stolen payment cards to purchase hard goods and then either intercept at the cardholder’s home or redirect shipment (either via the merchant or via the delivery service) to convenient pickup spots. This might be an abandoned gas station, the home of a complicit fraudster, or perhaps even a well-intended person stuffing envelopes as part of “work at home” schemes. They then sell these goods on the black market or ship them out of the country for more expeditious resale. At this point, merchants have not only lost expensive goods and face hefty chargeback fees and refunds; they often suffer lost sales as a result of their own goods sold on the grey market. This is particularly common among merchants dealing in higher-ticket merchandise (e.g., e-retailers, direct response merchants, etc.) that lend themselves to fencing (i.e. reselling stolen property) in secondary, underground, and overseas markets.

How can you mitigate package interception and redirection?

Authentication

Start simple. If you haven’t done so already, flag potentially risky orders (e.g., exceeding a particular value) for manual review prior to shipment. For those orders, consider contacting the cardholder directly to authenticate them and confirm their intent. Fraudsters won’t cooperate, but legitimate buyers will often appreciate the extra security.

The presence of a ship-to address in hard good orders increases the importance of authenticating customers. Require each customer’s billing address when accepting payment because, once confirmed, it serves as a good cross-check when evaluating the shipping address. It’s also helpful to verify the existence and permanence of the shipping address. For example, if you’re requested to process a shipment to a self-storage facility it’s likely a red flag.

Deviation

Good customers often request shipment elsewhere—to work, the home of a friend or relative, etc. More often than not, however, the destination will be reasonably close to the billing address. This isn’t always the case for those looking to redirect shipment as part of fraud attacks. Check the proximity of the shipping address against the buyer’s billing address, along with other order details. For instance, it would be suspicious for a customer living in Tennessee to request overnight shipment of a high-value product to an address in Haiti.

Repeat offenders may also reuse drop-ship points for the same reason legitimate businesses do—building reliable infrastructure is time-consuming and costly, even for bad guys. Take advantage. Implement a velocity check on each shipping address and flag those that exceed your cap. Pay even closer attention when a velocity check is triggered and you find the shipping address being used across multiple customers, payment cards, etc. Once again, that isn’t normal.

Reputation

It’s also very common for fraudsters to commit this particular attack across merchants. The complicated path from placing a fraudulent order to fencing-for-profit dictates that thieves place their proverbial eggs in several baskets. This is yet another reason to participate in shared, but anonymized, data pools coordinated by a number of third party providers. Check the reputation of shipping addresses—especially when associated with higher-value products—against your history and that of industry peers.

4 https://about.usps.com/publications/pub300a/pub300a_tech_022.htm
**NEXT STEPS**

After getting a better idea as to the fraud attacks and best practices common to the industry, the next question is how to start acting on some of these recommendations. There are several options, each with their own pros and cons.

You could enlist the help of a third party. Standalone fraud detection providers, aggregators, and value-added processors offer a variety of sophisticated, leading-edge tools and techniques. Alternatively, you could opt for the reliability and precise configurability of a home-grown system. For some, a hybrid approach is most appropriate.

Before making a decision, it’s important to keep the future in mind. Inevitably, incremental enhancements will be required on top of whatever is implemented today. With an organized and resourceful IT team, it may make more sense to take on the future configurability in-house. That would allow for close, constant surveillance of emerging threats, their impact, and potential defense in real-time. It’s also important to consider your access to shared cross-industry insight into the perpetrators of existing and emerging threats. Strong, established partnerships with peers will make a home-grown strategy more effective. On the other hand, if new vendor integration, shared intelligence, and sophisticated data analytics are not core competencies, it may help to engage third party experts.

The reality is that fraudsters are organized, persistent, and, worst of all—adaptable. They are adept at finding the most vulnerable points across the eCommerce landscape and taking advantage of them. The better you understand the specific nature of fraudster attacks relevant to your business and industry, the more informed you’ll be as you plan your next step.

For more information on how our proven eCommerce payment processing offerings can help your business acquire, convert, and retain profitable consumer relationships, contact our solutions professionals at 800-548-5326, or sales@litle.com.