Quatrro
Beyond the existing
PROCESSING SERVICES

Mitigating Fraudulent CNP Transactions

Examination of Safeguards

Electronic commerce has become a wildly successful channel for merchants and their customers. While the ability to shop online or through mail order catalogs is not new, the explosion of merchants with digital storefronts and the comfortability among consumers to shop there is growing. Consider Amazon a once fledging online book retailer. Revenues in 2012 totaled $61 billion up from $15 billion just 5 years prior. Other popular online retailers such as Walmart are seeing double digit year over year growth.

There is, however, a dark side to electronic and mail order storefronts. The explosion of these channels has opened the door to ever expanding card fraud. U.S. merchants lost $2.7 billion to online fraud in 2010, and over half of those surveyed indicated that fraud is getting harder to detect. In addition, only 40% of online retailers are taking any meaningful action to protect themselves from fraudulent buyers.

State of Card Fraud

The problem is here to stay. Over the next few years, more and more transactions will occur without the physical plastic, and by 2016 CEB TowerGroup projects that more than $2 trillion in transactions will likely come from channels where the card is not present. Now, if one applies a conservative 0.5 percent chargeback rate to the total, the annual value of chargebacks is estimated at $10 billion with about half of that estimated to be a direct result of fraud. This hits the bottom line with great effect.

The growth in electronic commerce has also led to changing patterns in card fraud. Where once counterfeiting and skimming were common fraudsters are now turning to online, mail-order and telephone-order channels to prospect their trade. Within these channels, no card is physically shown or swiped by the merchant thus they are termed Card Not Present (CNP) transactions. The move to EMV enabled plastic cards will only accelerate the shift to CNP fraud as it will become far more difficult for fraudsters to counterfeit cards. According to the CEB TowerGroup, in some cases, fraud can be 15 times higher in card not present transactions, versus when the card is present.

Clearly, fraudsters are becoming more sophisticated at mimicking legitimate cardholders in a remote or virtual-based transaction, and they are far less at risk of getting caught than doing so in a physical point-of-sale (POS) environment. CNP fraud also transcends geographic location. A catalog or e-commerce retailer can experience fraud from anywhere across the globe a feat not possible where a card is physically present.

Warning Signs of CNP Fraud

The bedrock of fraud mitigation is the use of advanced algorithms and detection systems to isolate fraud patterns and block suspicious transactions. However, simple warning signs can provide clues to help financial institutions and merchants better understand their vulnerability. Below are some common fraud indicators.

Large Orders. Stolen cards or account numbers are likely to have a short life span. Once the cardholder realizes his/her card account has been compromised they will move quickly to close the account. Card fraudsters will make large transactions quickly to maximize their opportunity.

Similar Orders. Card fraudsters will seek to purchase items that have good resale value often with large ticket amounts. These may include expensive electronics or jewelry. It is not uncommon for a card fraudster to purchase large quantities of the same item in rapid succession.

Rush Shipping. The crook will want to get merchandise out of the merchant's warehouse as quickly as possible in case the cardholder or card issuer identifies a fraudulent charge within 24-48 hours. Once the merchandise has been shipped, the merchant loses both the transaction and the value of the goods.

International Shipping. A large number of fraudulent transactions are shipped outside of the U.S. Pay special attention to purchase orders emanating from Nigeria, Belgium, Bulgaria, China and remote parts of Russia. Stolen account numbers are more common there.

Running a Card. Fraudsters often run multiple transactions on a single card account in a very short timeframe until the account is closed. In this scenario, a fraudster may purchase items online from different merchants rather quickly in what may be considered normal amounts so as not to raise suspicion.

Multiple Cards on Single IP Address. An Internet Protocol address (IP address) is a numerical label assigned to a computer device. An IP address serves two principal functions: host or network interface identification and location addressing. Keep in mind that multiple card accounts emanating from a single IP address could indicate a fraud ring.

Changing Email Addresses. A new customer that purchases from a merchant multiple times in a short period may change his/her email address with each new online checkout. In this instance, the crook is attempting to mask his identity.

Combating CNP Fraud

Understanding common CNP fraud is one thing, solving for it is another. There are a variety of methods to combat fraud. Cardholder education is typically the first step of a bank or card issuer's fraud prevention strategy. Providing cardholders with best practices in using and securing their plastic is

a common tactic deployed in card mailers. Disclosing the intrinsic safeguards built into the card is important for the cardholder to understand. However, this alone is not effective.

At the core are intrinsic methods for protecting cardholders. These methods use built-in features to authenticate a transaction. The most common are card security codes. These are three- or four-digit numbers printed (not embossed) on the card or signature strip, but not encoded on the magnetic stripe. Card associations use these codes with varying naming conventions: MasterCard (CVC2), Visa (CVV2), and Discover and American Express (CID). This is an effective method to combat stolen account numbers, but it does not solve for situations where the card itself was stolen.

One of the most common authentication methods is requesting card expiration dates in order to complete an online transaction. This authentication technique is widely used, and serves as another firewall to block against stolen account numbers. Yet again, this security measure breaks down in cases where the physical card has been stolen.

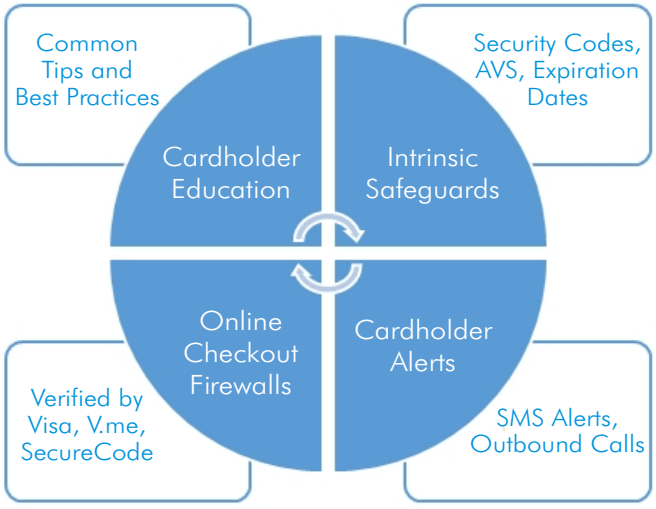
Another intrinsic method includes Address Verification Service (AVS). AVS matches billing address information provided at the online check-out with the cardholder's billing address on file with the card issuer. Upon authentication, the processing network sends an AVS response code indicating the results of the match to the payment gateway. Based on AVS rejection settings, the transaction could be accepted or rejected. Keep in mind that many non-U.S. banks do not support AVS verification. Therefore, AVS is not absolutely effective for limiting suspicious transactions from outside of the United States.

The card associations have created additional layers of protection. Recent methods developed include Verified by Visa® and SecureCode™ from MasterCard®. These require cardholders to present a personal ID in addition to their payment credentials at an online checkout. Another variation is V.me. Cardholders can store one or more of their cards in a special secured account. At online checkout, the cardholder clicks the V.me button, signs in with their email address and password, confirm payment details, and click pay. Keep in mind that cardholders and merchants must setup these services independently of each other in order to leverage the safeguards. And, a cardholder is not required to use these services so normal online card transactions still apply.

Card issuers have also deployed customer touch-points as a fallback. These may include SMS text alerts and outbound calling in cases where a transaction looks suspicious. However, in this case, the fraud has likely already occurred.

While these methods are effective at controlling fraud, they are not the only solution. Fraudsters have become very sophisticated, and these measures can crack under the weight of ever increasing fraud technology, and the sheer volume of activity likely to occur in the coming years.

Typical CNP Fraud Prevention Strategies



Next Generation CNP Fraud Detection

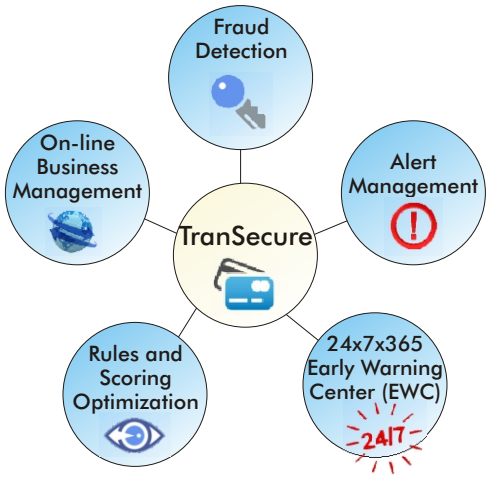
There are many tools to safeguard CNP transactions with some being more effective than others. The challenge banks and issuers have is melding these fraud mitigation tools into a cohesive strategy that limits resource constraints born from the day-to-day monitoring of suspicious transactions. Decision management software such as FICO® Falcon® provide global protection against card fraud. This system uses advanced algorithms and rules to auto detect irregular patterns and suspicious transactions that limit false positives.

The reality is that automated systems are not totally secure. Even with advanced fraud mitigation technology, fraud still occurs and cardholders' lives are still disrupted. Technology alone can create a false sense of security for both the merchant, issuing bank and the cardholder. Effective mitigation strategies combine both the technology and software with large teams of fraud analysts who are monitoring, rewriting parameters and blocking transactions that are flagged by automated systems as suspicious.

This layered approach provides a highly effective firewall to protect and secure card transactions. What is often not provided, especially for small to mid-tier banks and credit unions, is access to highly seasoned fraud analysts who monitor and resolve instances where typical automated detection systems fail. Small to mid-tier financial institutions often cannot afford or staff appropriately to handle ever increasing and ever sophisticated card fraud attacks. Until now.

At Quattro Processing Services, our core strength is the layer of human intelligence our risk specialists bring to fraud analytics and operations. We analyze high volumes of data, uncover trends and anomalies, and revise processing parameters and rules that tighten the noose on card fraud.

TranSecure™ from Quatrro Processing Services is a powerful Card Not Present (CNP) business enhancing and fraud reduction tool. It is a comprehensive application which



leverages the transaction information to generate alerts as well as business intelligence reports. It also provides merchants and financial institutions with a dynamic user management interface which can be used to adapt to the changing payment environment on a real-time basis. This technology is layered with human intelligence. A host of fraud analysts are reviewing suspicious transactions that enter TransSecure serving as a powerful filter to compliment the automated rules engine.

Quatrro Processing Services can also correlate suspicious activity with customer behavior across multiple electronic transaction channels. Our analysts scan activity 24/7, utilizing various instruments across all banking channels.

Even if an institution has separate technical systems for each product set, our team can connect these subsystems to manage cross-channel fraud, using a financial institutions existing fraud tools. Our approach allows us to scale up easily, improve bottom lines quickly, and evolve with financial institutions to combat new threats. Unlike our competitors, Quatrro provides a holistic approach to managing risk across the full transaction cycle with both technology and human interfaces.

Quatrro Processing Services monitors and blocks all fraud types. Our services cover ID theft, cross-border fraud, account takeover, lost/stolen cards, Card Not Present fraud, and skimming and counterfeiting. And our expertise is grounded in fact: for every $1 a financial institution invests in Quatrro Processing Services risk management services they receive a return of $30.

Accelerating CNP Fraud Prevention: Quatrro and NorseCorp A Powerful Combination

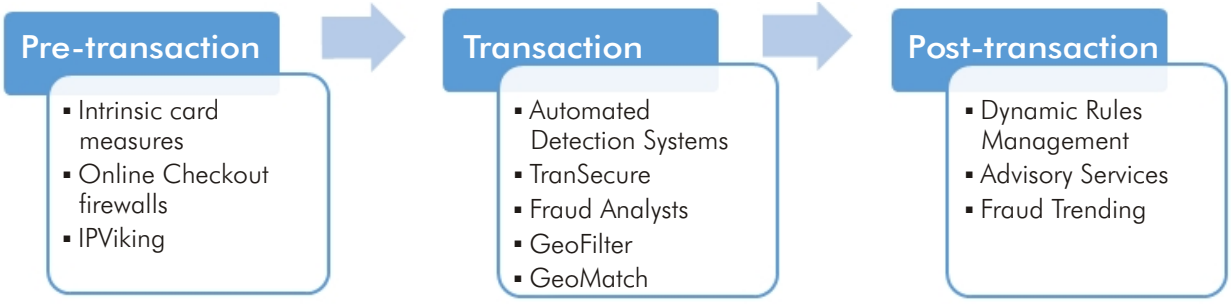
Quatrro Processing Services takes fraud management even further. Through a partnership with NorseCorp™, a leading provider of live cyber risk intelligence and fraud solutions for businesses, Quatrro Processing Services will provide industry-leading fraud detection through the entire transaction lifecycle even cutting card fraud before a transaction actually occurs.

Banks and Credit Unions. Quatrro Processing Services can track IP address locations of card fraudsters across the globe using NorsecCorp's IPViking technology. We can block transactions from select countries, zip codes and IP addresses so the transactions never have a chance to route through the payment network. Our real-time reporting alerts merchants before the item is shipped saving untold dollars. The ability to stop fraud before it has a chance to manifest is real peace-of-mind for financial institutions, merchants and cardholders.

IP address monitoring through IPViking can also solve for common bank transactions like check deposits. With Remote Deposit Capture (RDC) banks and credit unions can be assured that checks deposited are legitimate transactions from customers or members. Counterfeit checks being deposited from high-risk zip codes, high-risk foreign countries or suspicious IP addresses can be blocked before they have a chance to route through a financial institution's system.

Hackers and spammers are constantly working to compromise online banking channels often disrupting account access through a distributed-denial-of-service attack (DDoS) that can last for hours. Financial institutions need to ensure continuous and uninterrupted access to online channels or they risk damaging coveted loyalty and relationship statuses. IPVenger protects web sites and content from hackers, spammers, and malware. It automatically assesses the risk level of every visitor in real-time, proactively blocking hackers, bots, malware, and comment spam before it has a chance to enter a financial institution's site. IPVenger provides live security analytics and visualizations of a site's traffic based on proprietary IPQ risk scores, threat categories, country of origin, and other risk variables.

Effective CNP Fraud Management Process Layered Approach



Merchants. IPViking provides merchants the most current and advanced intelligence about fraudulent IPs and devices available today. Unlike competing products that only provide scoring after a fraudulent event occurs, IPViking scours the Internet 24/7 monitoring over 2.1 billion IP addresses and gathering intelligence on IPs and devices likely to commit fraud. It utilizes millions of active and passive sensors deployed across the globe in over 30 datacenters that analyze terabytes of suspicious traffic per day. The data captured is then used to create over 100 factors which

are used to calculate NorseCorp's proprietary IPQ risk score within microseconds. NorseCorp's IPQ score provides merchants with a simple but powerful tool to assess risk levels and make decisions and make decisions to prevent fraud before the payment transaction is executed.

In addition to the IPQ score, IPViking utilizes GeoFilter and GeoMatch features to provide the merchant with country, city, state, billing address and zip code offering the merchant additional decision data points. The GeoMatch feature takes the geo data points one step further by providing a risk factor based on the calculated distance in miles between the billing address and IP address location. GeoMatch provides a level of added security for all parties as a fraudulent transaction will be stopped in early detection before card authorization. It also assists a merchant in dealing with customer support issues arising from "Friendly Fraud" where a customer claims a transaction was not done by them or family member.

The combination of Quatrro Processing Services and NorseCorp provides a powerful enterprise-wide risk management platform covering each stage of the transaction process with a powerful solution against hackers and spammers. Quatrro Processing Services provides the secure payments vault that financial institutions need to combat the ever growing presence of card fraud.

Conclusion

Fraud costs businesses billions of dollars each year and wreaks havoc in the lives of its victims. Financial institutions need a solution that protects their customers across the entire transaction lifecycle regardless of channel or point of entry. As fraudsters grow more sophisticated so should a financial institution's risk management tool box. Only then can they be confident in knowing their cardholders are genuinely secure.

About Quatrro Processing Services

Quatrro Processing Services provides an innovative approach for your credit, debit and prepaid card processing needs. Our portfolio processing solutions are delivered by a non-legacy platform that offers a flexible and customizable alternative. Quatrro also offers an integrated suite of managed services across the entire risk cycle spanning credit, fraud and portfolio management. By leveraging our Analytics and Transaction Monitoring solutions, your organization can more effectively manage your core competencies resulting in increased cost savings, streamlined operations and improved business processes.

For more information please visit: ***www.quatrroprocessing.com***

About NorseCorp

Norse is a leading innovator of IT security and fraud prevention solutions - and the only provider of live, actionable, cyber threat intelligence. Their patent-pending IPViking technology continuously monitors the Internet for hacker activity and high risk network traffic. Using proprietary big data analytics of the internet's high-risk traffic, IPViking enables companies to prevent financial fraud, enhance network security and protect against security breaches. From enterprises to developers, NorseCorp enables live, proactive, security and anti-fraud solutions for websites, applications, e-commerce systems, and network devices.