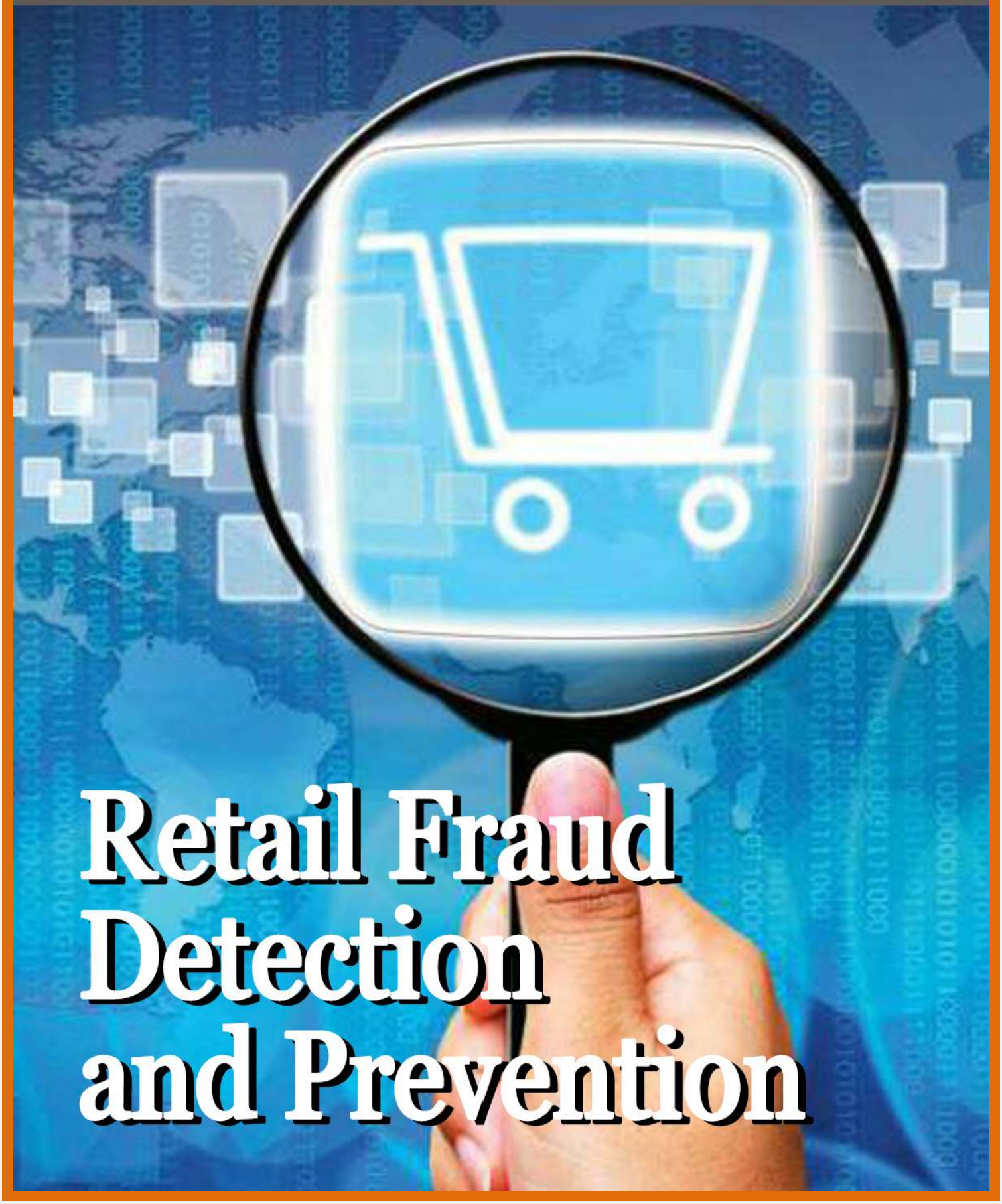
LPM SPECIAL REPORT



Retail Fraud Detection and Prevention

Cyber attacks and data theft are making headlines like never before, with some of the largest and most well-known brands—Target, Home Depot, Sony, Anthem—falling victim. With the frequency and pervasiveness of these attacks, executives in companies of all sizes and across industries are left asking, "If these businesses can be compromised, are we next?"

But rather than being consumed by fear, uncertainty, and doubt, it's time to be constructive and proactive to address these attacks. The new reality is when, not if, a data compromise will occur. Embracing the fact that these criminal acts are lucrative and difficult to prosecute has created a new paradigm in the retail landscape. As long as computers and the Internet serve a central role in commerce, these attacks are not going away.

POS: A Major Target

In recent years, there has been a tremendous amount of data leakage from retailers that have had their payment-card systems compromised. This not only includes credit card information stolen from the point-of-sale (POS) registers or terminals, but other sensitive customer information as well, such as address, date of birth, telephone number, email addresses, and more.

Statistics show that 50 percent of the readers of this article have had to replace one or more credit cards in the last eighteen months due to a point-of-sale hack. This is of great concern, to say the least. In 2014, the FBI issued an alert to retailers indicating that we had seen just the tip of the iceberg as far as the emergence of malware designed to penetrate and capture our sensitive data. True to this warning, more and more infections and security breaches regarding POS systems have been reported since then.

The good news is that the situation isn't hopeless. However, it does require proper planning and investment in new approaches to skill development and technology implementation. It also requires innovative ways to deconstruct and analyze how these targeted attacks evolve within your networks.

Payment Card Data Theft

Stealing payment card data has become an everyday crime that yields quick monetary gains. The goal is to steal the data stored in the magnetic stripe of payment cards, (optionally) clone the cards, and run charges on the accounts associated with them. Criminals have been physically skimming payment cards, including both debit and credit cards, for years now. Common techniques for skimming payment cards include:

- Making a rub of the card
- Rigging ATMs or gas pumps with fake panels that steal data
- Modifying store POS terminals
- Using off-the-shelf hardware keyloggers on cash registers

These techniques all require physical access to the cards or the devices used to process them. This introduces a high risk of getting apprehended. Plus, skimmers cannot be readily mass deployed for maximum effectiveness. Therefore, criminals have begun changing their focus to using malicious software to steal payment card data—primarily credit card data.

Credit Card Hacking 2.0

POS RAM scraping is a software methodology for stealing credit card data. After the merchant swipes the credit card, the data on the card temporarily resides in plain-text format in the POS software's process memory space in random access memory (RAM). The magnetic stripe on the back of the credit card contains three data tracks. Credit cards use the first two. When the credit card is swiped, data from these tracks are read into the POS software's process memory.

How Do Hackers Infiltrate?

Retailers and other businesses that process credit cards, irrespective of their size, are data-theft targets. The most convenient place to steal credit card data is from the RAM of POS systems where the data temporarily resides in plain-text format during transaction processing. The challenge for cybercriminals is to find a reliable method to infect POS systems. Some of the common infection methods are described below.

Inside Jobs. The inside job is the most difficult infection vector to prevent, since it involves people whom businesses trust or those who can abuse their privileges to commit crimes. These could include disgruntled or disillusioned employees out to take revenge or even just unscrupulous individuals out to make quick cash by victimizing their employers.

Phishing and Social Engineering. POS RAM scrapers are never spammed out to millions of potential victims. Instead, they are sent to a chosen few targets via phishing emails with effective social-engineering lures. Small businesses often use their POS servers to browse the Internet and check email, making them easy targets for phishing attacks. It's not a bad idea for loss prevention professionals to look into developing company policy against using POS servers this way.

Vulnerability Exploitation. New software vulnerabilities are disclosed and patched every month by their respective vendors. Only a handful of these

are successfully "weaponized." Once weaponized, the vulnerabilities will be used in cyberattacks for years. These exploits are able to successfully compromise systems when IT has not rigorously applied these vendor patches. The reality is that many POS servers are still running outmoded, unsupported operating systems.

PCI-DSS Non-compliance Abuse. The Payment Card Industry Data Security Standard (PCI-DSS) refers to a set of requirements designed to ensure that companies that process, store, or transmit credit card information maintain a secure environment. PCI-DSS does not offer new secure technologies to protect electronic payment systems. It does provide requirements to build up additional layers of security controls around controls that already exist. Hardening systems and networks (making them more secure) is not a trivial task. Companies that lack expertise or resources often incorrectly configure their POS environments, making them susceptible to malware attacks.

Targeted Cyber Attacks. Targeted POS RAM scraper attacks are attacks aimed at large businesses with millions of credit cards. There are six different stages of these attacks, from ensnaring a victim to exfiltrating stolen data to the black market. Some of the most malevolent attacks of all, these targeted assaults are meticulously planned and well executed, making them notoriously difficult to detect.

POS RAM scraper malware retrieves a list of running processes on the victim machine, loads each process's memory space in RAM, and searches for the credit card data residing there. The malware scrapes the payment card data from RAM and exfiltrates it to the cybercriminals. The stolen tracks' data can be used to physically clone the credit card or can be used in fraudulent card-not-present (CNP) transactions, meaning online purchases.

Promoting Security beyond Compliance

POS security can no longer be a checkmark on an audit to-do list. It has become a business driver—an integral component of business operations. Proactivity is a must because every business that possesses or processes credit card payments is a target for POS data theft.

To effectively protect against POS RAM scraper attacks, businesses need to protect all aspects of their operating environments, not just the POS systems. Attackers can gain initial entry into the corporate network using compromised credentials or via phishing emails. From there, they can locate the POS systems and infiltrate them.

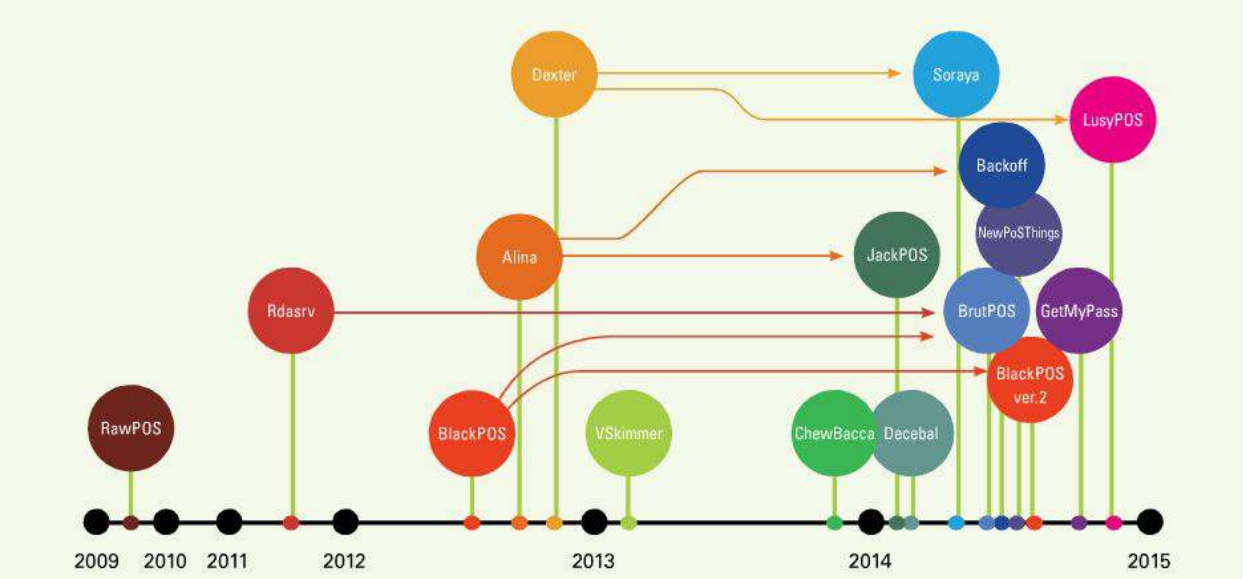
The key to setting up a strong defense is to understand the nature of the threat. In the case of POS RAM scrapers, this means understanding the malware's attack chain. Through countless hours of research, security analysts have been able to see trends and patterns on how these attacks persist and, ultimately, the success that they have in stealing sensitive data.

As companies formulate defense strategies, they should keep in mind the following:

- Size of the organization—Large organizations have complex networks with thousands of connected devices, multiple locations, and so on. Security solutions must be scalable, centrally managed, and able to defend complex networks.
- Costs—Security solutions can become expensive, especially when the organization requires multi-tiered defenses. Businesses should factor in the costs of in-house and/or externally contracted IT services required to manage the deployed security solutions.
- Multi-platform support—Many businesses support several major operating system (OS) platforms in their operating environments, so security solutions must be able to protect all of them and provide centralized management of the protected devices.
- Bring your own device (BYOD)—Organizations are increasingly moving toward implementing BYOD policies as a means of cutting costs and giving employees flexibility. BYOD policies introduce new challenges regarding securing employee-owned devices that are accessing the organization's resources.
- Consumers and end users will also have to adopt a "shared-security" attitude—This includes taking steps to ensure that their BYOD devices are protected. As we move to a more frictionless form of payment capability, we must ensure that the devices that we enable to carry out these payment transactions are pristine. We will also have to embrace multi-factor and biometric capabilities to help thwart future attacks.

Time for Forward Thinking

Implementation of EMV (Europay, Mastercard and Visa) chip-and-PIN technology as well as next-generation payment platforms and e-wallet capabilities will certainly help reduce POS attacks, but won't guarantee the complete elimination of payment attacks. Retailers and financial institutions need to work diligently to determine the possible failure modes of their own systems.



History of POS RAM Scraping

The earliest evidence of POS RAM scraping was in the Visa Data Security Alert issued on October 2, 2008. Back then, cybercriminals attempted to install debugging tools on POS systems to copy credit card data from RAM. POS RAM scrapers have quickly evolved since then to use multiple components and exfiltration techniques.

To get a better perspective of the evolution of POS RAM scraper malware families, see the timeline diagram above, organized by year of discovery. Note that a malware variant may have existed long before it was discovered, so it is difficult to track exact dates. Although most people may not have heard of these malware variants, this diagram will still show you how the frequency has continued to increase over the last several years.

A couple of notes regarding the timeline diagram:

- Seven unique POS RAM scraper families were discovered between 2009 and 2013.
- Nine unique POS RAM scraper families were discovered in 2014 alone.
- The arrows connecting the bubbles indicate either a direct evolution or technology reuse.

Retailers should be spending money on creating rich POS payment applications that are securely tied to our mobile devices and that can leverage cheap technology to process and transmit transactions. This may be preferable to spending hundreds of millions or billions of dollars implementing chip-and-PIN technology that will be cumbersome for consumers to leverage in two to three years (if not sooner). At the rate that this technology is advancing, this form of payment will be outmoded quickly. We should demand more from our companies and challenge them think much bigger.

In January 2014, the FBI warned that we hadn't seen the end of the POS breaches. The agency was correct. Target, P.F. Chang's, UPS, Home Depot...the list continued to grow and hasn't stopped yet. Dozens of other organizations that process payments have fallen victim to targeted attacks. It's time to be forward thinking about where this market is going and spend money on the right payment platform that will scale for the masses for the foreseeable future.

It is crucial for retailers to implement breach-detection capability to deconstruct and analyze suspicious campaigns. Finding out about a breach sooner rather than later means maximizing the chances for damage control. Knowing is 90 percent of the battle in stopping exfiltration in your organization.

As a loss prevention professional, it's not beyond your scope to ask your IT department hard questions about what they are doing to prevent these thefts. In fact, every employee should feel comfortable asking these questions. In today's climate, we truly are all risk managers.

EMV

EMV, known in the UK as "chip-and-PIN," is a global standard that strengthens card authentication using a computer chip physically built in to the card. Instead of reading card data off the card's magnetic strip, every time a customer inserts their chip card into an EMV-equipped POS card reader, the chip generates a new, unique transaction code. Since the magnetic strip data remains the same with every use, copying that data by card skimming or stealing it in a hack allows the account to be imprinted on

counterfeit cards or reused illegally online. But chip-generated codes are one-time use only—stealing one becomes useless.

For the UK, chip-card deployment was largely successful in reducing domestic face-to-face card fraud, but there was a dramatic rise in foreign fraud using UK-issued cards, as well as card-not-present card fraud. "When the UK went to chip-and-PIN, there was a spike in online fraud," said Scott Sanford, director of investigations for Barnes & Noble. "The brick-and-mortar card fraud migrated to the online world."

On October 1, 2015, the U.S. payment card market will make a similar move. On that date, the liability for card-present counterfeit card losses will shift from issuer to merchant unless the merchant implements EMV. In effect, what this liability shift means is that by the end of this year most consumers' cards will have a chip in them and most brick-and-mortar merchants will be processing cards by reading these chips instead of the conventional magnetic strips, making in-store card counterfeit fraud much more difficult.

While in-store card fraud may fall significantly, many expect online card fraud to jump in response, as it did in the UK. "If brick-and-mortar credit card fraud is my game, and I have EMV potentially blocking my lifestyle, I'm going to go try to do it online," said Sanford. "I think online fraud is going to jump dramatically in the US." Even were it not for the EMV adoption, some experts expect online fraud would continue to increase over the next one to two years. So although major strides have been made over the past decade, e-commerce fraud is still a significant challenge to the LP industry today and will remain so into the near future.

Introduction to Online Fraud

In the world of fraud prevention, there is a thriving, underground economy of web-savvy criminals who are knowledgeable about card-not-present (CNP) fraud and how to exploit merchant vulnerabilities for personal gain. The unfortunate reality is that criminals are stealing consumers' credit card information, either in the physical world or via online phishing attacks, and selling it on the Internet.

Sophisticated fraudsters, who are increasingly well organized and working frequently from outside the U.S., obtain the card number and security code data to buy popular merchandise over the web and then resell it for profit. Perhaps less sinister, but just as problematic, are family members using credit cards to make unauthorized purchases.

CNP fraud involves nameless, faceless crimes that are difficult to trace and prosecute. Fraudsters steal consumer identities and operate in rings to cover their tracks. They are adept at evolving their schemes to elude merchant controls and are constantly looking for ways to remain under the radar. For instance, many merchants review orders that request express shipping because many such orders have been linked to fraud. Knowing this, a fraudster might request standard shipping on a purchase then call customer service a day later complaining that the order was processed incorrectly. Without proper prevention techniques, the fraudster gets overnight delivery of the package without tripping merchant fraud alerts.

Although major strides have been made over the past decade, e-commerce fraud is still a significant challenge to the LP industry today and will remain so into the near future.

Examining Charge-Backs

The first step to prevent fraud is looking at a company's charge-backs, a frequently cited metric for online payment fraud. Charge-backs are a sale reversal that occurs when a customer claims their credit card was charged for a purchase they didn't make. The typical practice for many retailers is to supply information requested by the card issuer and to write off the loss as bad debt.

But it's important to adopt measures for reducing charge-backs because they are costly and eat away at a retailer's bottom line. The retailer loses the full value of the merchandise and also incurs a charge-back penalty from the card issuer. A company with a high charge-back rate risks heavy fines or being dropped by card issuers.

There are two things that retailers can do to minimize these losses. The first is to dispute charge-backs in an effort to reverse them. This isn't easy, as the burden is on the merchant to prove that the merchandise was received by the cardholder, but you

are likely to succeed in reversing a certain percentage of them, which will save your company money. The second, and more effective thing you can do, is to prevent charge-backs before they happen, which means identifying incoming fraudulent orders and cancelling them before the orders are fulfilled.

Many retailers have automated order-screening systems for exactly this purpose. For example, if an order exceeds a certain dollar amount, or if the billing and shipping addresses don't match, the order may be flagged as potentially fraudulent and placed into a review queue in the order management system for further inspection by a fraud analyst. A "negative file" of order data, such as email addresses and physical addresses associated with past fraudulent orders, may also be maintained. New orders involving any of these negative data elements are also queued for an analyst's review. In addition, retailers can monitor for order velocity, meaning customers placing similar orders in succession over a short period—another hallmark of fraudster activity.

Performing a detailed analysis of charge-backs on a historical basis can help determine what kind of fraud was slipping through and how controls could be improved. An in-depth look at charge-back data could provide valuable information about the nature of fraudulent transactions and could enable retailers to fine-tune fraud controls based on fraudster behavior.

What Does e-Commerce Fraud Look Like?

"Compared to the professional shoplifter teams of years past who come to stores and shoplift in groups or do basic grab-and-runs, the types of ORC actors you see today are very sophisticated," said John Matas, vice president of asset protection at Macy's. "These groups have the traditional organized crime hierarchy, and the higher the level within the group, the more insulated an individual is from arrest. These groups are well organized and highly technical, taking full advantage of all sorts of retail processes designed to enhance our customers' shopping experience, but in a criminal way."

For example, the realm of gift cards has its own subgenres of gift card fraud. Legitimate websites intended to store gift cards on your phone have been used by criminals to launder stolen cards. One group broke the mathematical algorithm used to generate gift-card number/PIN combinations, then manufactured actual counterfeit plastic cards to use them with.

"Friendly fraud" is another problematic category of fraud. Friendly fraud is when the actual cardholder (or somebody known to the cardholder) makes a legitimate purchase, but then tries to dispute the charge by claiming they never made a purchase or never received the merchandise. These are difficult cases for a merchant to challenge.

Of the many types of fraud in existence, the triangulation scheme was ranked the ninth most impactful type of fraud in 2012 based on frequency of attack and revenue loss; by 2013 triangulation had jumped to the number one perceived threat, according to a survey conducted jointly between the Merchant Risk Council and CyberSource.

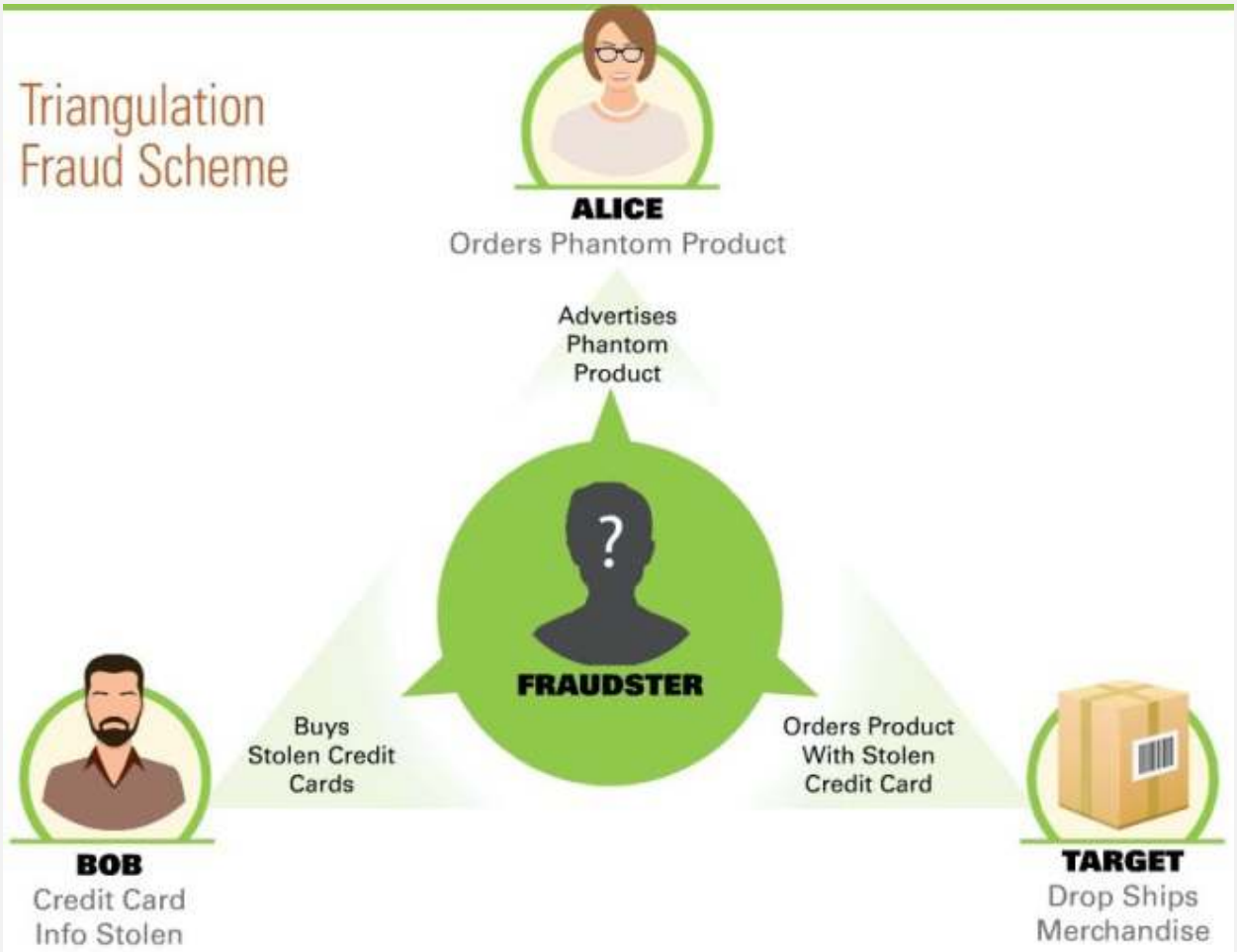
Like many online frauds, the triangulation scheme starts with obtaining stolen credit card account information. For that, the best place to visit is the Deep Web, the name for those realms of the Internet you can't get to from a Google search. Some parts of the Deep Web are still a Wild West, free from regulation, and may only be reachable using specialized software that masks users in anonymity.

Triangulation Fraud Schemes

So our fraudster—we'll call him Chuck—has gone to the Deep Web and bought a few thousand complete credit card account records, including cardholder name, billing address, credit card number, CVV security code, and possibly corresponding email addresses, phone numbers, and other personal information.

The next step in the fraud is listing an item for sale on an online marketplace, such as Amazon, Craigslist, eBay, or any of the thousands of other online auction houses and marketplaces. Nearly any category of merchandise will do—books, clothing, or electronics—as long as the product is in relatively high demand. Chuck decides to list a brand-name laptop for sale. In order to quickly find a buyer, he has to list that laptop at a price point below that of the legitimate sellers out there—if he didn't, customers wouldn't have any reason to buy from him over any big-name retailer. The laptop retails at $150, so Chuck (connected through a proxy) posts a listing on eBay for a brand-new laptop for $125 plus free shipping.

Alice is shopping for a laptop. She's a crafty consumer. She wants to save money. So instead of buying at full retail price, she shops around. She searches eBay, sorts the results by lowest price, and there is Chuck's listing right at the top. "Wow, what a deal," she thinks. Alice buys the laptop, and money is transferred from her credit card to Chuck's PayPal account. Chuck has never been in possession of the laptop. But he can't just ship nothing to Alice because she would leave negative feedback, file a complaint, and Chuck would find his eBay and PayPal accounts banned. So he has to send her the item she bought. In fact, he wants to appear not only as legitimate, but also as a high-quality, customer-satisfaction-focused seller.



So he goes to his list of stolen credit card accounts and pulls the first one on the list, which belongs to Bob, the legitimate account holder. Using a proxy server, Chuck visits Target's online storefront to buy the laptop. He uses Bob's credit card number and billing address, but enters Alice's shipping address. And then he submits the fraudulent order. Target processes the order and ships Alice the laptop.

Bob is the first victim—he had a fraudulent purchase made on his card. Target is the second victim—it will be hit with a chargeback. And Alice is the third victim—her name and address are on the fraudulent shipment. Thus the triangulation scheme came to be named for these three victims.

Chuck will use Bob's account only once or twice, and then he'll drop it and move on to one of the other thousand he has on hand. Target is looking at a $150 loss, so it doesn't make sense for its team to investigate it. Law enforcement, on top of looking at such a small loss, can't figure out who Chuck is since he's been using a proxy server. Both Target and law enforcement might dismiss the whole affair as a minor crime, but Chuck is doing this ten times a day with ten different retailers, on each of four different eBay accounts. In reality, there is large-scale fraud going on, but the online medium obscures the fact.

Combating the Triangulation Scheme

Of course, retailers have sophisticated ways to detect fraudulent orders. There are many red flags that could hint that an order is fraudulent, but these are almost never definitive—they merely add some probability that the transaction in question is suspect.

One way that many merchants and third-party fraud prevention vendors combat fraud is by putting every online order through a screening algorithm to look for these red flags and determine how likely it is that an order is fraudulent. These algorithms will frequently have hundreds of very specific criteria they check for. If the order fails one of the checks, the order is flagged with a certain number of fraud alert points commensurate with the likelihood of that criterion being associated with fraud. If the order passes a certain point threshold—say 1,000 points—it is sent to an analyst for manual review.

There are the obvious checks: is the shipping address different from the billing address? If so, add

200 points. Is this the first time this card has been used on the site? If so, add 50 points.

Then there are less obvious checks: are the first and last names capitalized? If not, add 200 points. (Apparently many criminals habitually enter names in all lowercase.) Did the transaction occur late at night? If so, add 50 points.

Then there are more subtle checks: is the transaction placed from a browser configured for a language from a high-fraud country? If so, add 100 points. Does the order originate from a proxy's IP address? If so, add 400 points. Is the proxy's IP address out-of-country? If so, add 200 more points.

Another fraud test is called "device fingerprinting." When you visit any website, various bits of information about your computer are shared, such as time zone and type and version of browser and operating system. This information can be analyzed to "fingerprint" an individual device. So if a fraudster is placing multiple fraudulent orders from behind multiple proxies to avoid detection, device fingerprinting can tie together several suspicious orders to reveal that they all came from the same machine.

Order velocity is a metric that can be used in a similar way. Velocity measures how often the same card is used to place orders on a site. Depending on the item and the merchant's customers' normal buying habits, multiple purchases in a short time frame can also point toward fraud.

If an order passes the 1,000-point alert mark, or fails any of the other tests, it gets marked as "suspect" and kicked to a human fraud analyst for review. Analysts have a number of tools at their disposal to help determine whether they should cancel the order or let it go through. They may pay for a public records search to validate order data. They may check social media sites or Google Maps. But they'll often just call or email the contact information given when the order was placed.

Balancing the Customer Experience

Fraud prevention is a careful balancing act. Weighting too heavily on the side of fraud prevention can negatively impact the customer experience. Asking customers to provide extra information at checkout for validation purposes will at best slow down the transaction, and if done improperly could make customers uncomfortable. And while contacting a customer to verify a purchase might be a positive to some ("this merchant cares about my security"), it could be a negative to others ("this call reduces the convenience of shopping online").

The last thing a retailer wants to do is drive away legitimate customers who were trying to make a purchase. "There are a lot of merchants out there," said Tim Guastaferro, director of e-commerce for Sears, "so if you take steps that make it anything but a seamless transaction, you run the risk of driving that customer to other sites where they don't have to jump through hoops. It's not all about fraud losses. We have to balance fraud losses with our customer experience, our operational expense, the ability to take on more payments, to offer more fulfillment types. We want to beat everyone to the scene on implementing these things because they are about enhancing the customer experience."

"There are tools out there that you can layer on your existing e-commerce platform to drastically reduce the chance of fraud. We could nearly eliminate it," said Jerett Sauer, director of loss prevention at Gap Inc. "That's not the issue. The issue is that you would highly impact your customer experience. The balance in how you are trying to structure your program becomes key. You want to make it seamless to 99.9 percent of legitimate customers, but make it just hard enough for fraudsters that they decide to go elsewhere."

Looking forward, a middle ground might be found in an access control concept called two-factor authentication. ATM withdrawals use two-factor authentication. They require something that a user physically possesses—the debit card—as well as something that a user knows—the PIN. For card-not-present transactions, the first factor—what they have—would be entered as it is now, manually typing card account information. The second factor—what they know—could be integrated by sending a text message to the mobile device number on file at the card-issuing bank. Since most people keep their phones on them most of the time, confirming a legitimate purchase using a phone could become an accepted non-intrusive step in making an online purchase that could dramatically reduce online fraud. Retailers, or retailer associations, cannot implement two-factor authentication unilaterally. It requires buy-in on the part of card companies and card issuers. But some expect this option to be regarded highly by the payment card industry in the near future.

Investigation

The role of the fraud analyst is inherently defensive. Analysts manually review orders that a merchant's automated fraud prevention system deems suspect. "Analysts can stop an order in its tracks, recall it, or allow it to go through," said Sanford. "But stopping the order doesn't dissuade the bad actor. They simply move on to the next retailer or the next card number, modifying their approach to fly under the radar the next time. One thing is certain—unless they're caught, the online fraudster will

continue their efforts one transaction at a time, one credit card number at a time."

But it is possible to track down these people, and that's where the investigator comes in. "It starts with the will to find them," said Sanford, "And it requires a collaborative effort on the part of many players, including online resale venues, banks, ISPs, law enforcement, and sometimes others." eBay has set the gold standard for this collaborative effort, according to Sanford. "Every major player engaged in peer-to-peer selling could learn something from eBay. They clearly want nothing to do with criminals engaging others on their site," he said.

One way for a retailer to track down fraudulent sellers is to search online marketplaces for products listed as new but offered at a price below what the retailer is paying for the product. One instance could be a fluke, but if a seller's sales history shows a pattern of similar offerings, the investigator has most likely found a fraudster. How they proceed from there depends on which marketplace the item is listed under.

Law enforcement won't look at a case unless it's a proven fraud event. Investigators can collect a great deal of evidence, but in order to get the final proof and identity information, they need information from the online marketplace. "My team and I have successfully conducted hundreds of investigations over the years," said Sanford. "Many of these investigations were concluded in partnership with eBay's PROACT team. Though we've also closed numerous investigations involving nefarious Amazon sellers, we've taken that trip solo, not by choice either. On the contrary, at least eBay has the decency to respond and show concern for society as a whole. They recognize that we all lose out when the criminal wins."

Working Together

Taking down cybercriminals is more difficult than just piercing the veil of anonymity to track down who the perpetrator is and where they can be found. "Prosecuting has always been a challenge," said Sauer. "Early in my career, it was almost impossible since you were usually looking at different parts of the crime being committed in different jurisdictions." Where a package was shipped from, where it was shipped to, the address of the merchant, the address of the stolen credit card's legitimate owner—these locations may be in entirely different states, or even different countries. And that's not even considering the location details of the criminal (or criminals). When considering a fraud scheme that has moved hundreds or thousands of items, each one with multiple different location components, the number of jurisdictions involved can multiply to a staggering number.

And the magnitude of loss is often concealed by using multiple accounts and targeting multiple merchants. "If I'm looking at $100 or $1,000 loss from one particular incident," said Sauer, "even if I know exactly who the perpetrator is, it's not worth my time or the authorities' time to prosecute, even if I've been hit multiple times. Most cases don't go above low double-digit thousands as far as loss." But if a criminal has hit a dozen other merchants in a similar way and has committed the same frauds using several other accounts to minimize his risk, one merchant's perspective may be just one piece of a much, much larger puzzle.

"If I get hit one night," said Sears' Guastaferro, "there's a good chance that another retailer has been too. So if I communicate with another retailer and they say, 'We know those people; we know that MO,' it does make it easier since we can put together a larger case."

The value of collaboration with other retailers has led to the formation of organizations for that very purpose. "We depend heavily on these organizations for networking and sharing of common ORC offenders," said Matas. "The most effective are the regional ORCA organizations. There are over twenty-two of these regional coalitions nationwide. Since the ORC and e-commerce fraud phenomenon has spread far beyond the local criminal groups—there are national and international linkages—the next logical step is tying these regional ORCA coalitions into one master national association and creating a unified national ORC database. Together, our ongoing ORC investigations and prosecution dollar value could be significantly larger when it comes to federal prosecution."

As our modern digital lifestyles become further intertwined with the physical world, it becomes increasingly important for us to remain aware of the benefits this marriage brings and vigilant of its risks. The complexity of modern digital systems is staggering and continually increasing, making it more and more difficult for any one individual to be able to truly understand how all the pieces fit together. Since increasing system complexity is associated with an increase in the number of possible failure points in the system, total risk exposure increases unless we remain proactive. Fraud affects individuals just as it does companies and the greater industry, and just as the industry and the company are collaborating and evolving to combat these modern threats, so must we as individuals.

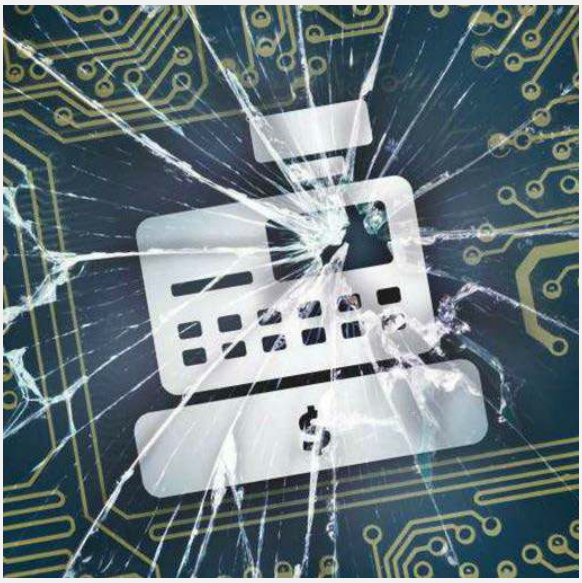
Best Practices

Following is a summary of recommendations and best practices that can help you reduce charge-backs and cut overall fraud-related losses.

- Completely eliminating CNP fraud isn't a cost-effective strategy. A good fraud prevention program should be designed to minimize your company's exposure while allowing legitimate customers to purchase with ease.
- Analyze your charge-back data historically and on an ongoing basis. Analyzing the data elements associated with fraudulent charge-back orders will help you determine if your fraud controls or procedures need tightening.
- Challenge your charge-backs. Merchants that do so recover on average more than one-quarter of their fraud charge-backs.
- Today's order-screening systems have become more sophisticated. Choose one that can detect more complex fraud patterns while allowing you to give more weight to certain rules and scoring to calculate the overall risk of each transaction.
- Create negative files for checking orders based on rejected transactions and fraudulent orders that resulted in charge-backs, keeping them updated automatically. Also create positive files from data in your customer records so you won't delay orders from legitimate customers when their buying habits innocently make them appear risky.
- Your fraud solution should be designed to permit non-technical users and fraud managers to modify your controls and deploy new ones.
- A comprehensive fraud solution should automatically sort, rank, and prioritize suspect orders so analysts can stay focused on the riskiest orders and orders that need to be shipped quickly.
- Automate your review process to the fullest extent possible.
- Use multiple tools to identify fraud. A fraudster that successfully bypasses the address verification service (AVS) or card-verification-number (CVN) checks may be caught by device identification, identity verification, or geo-location technologies.

Your fraud solution should readily accommodate plug-in of new tools and third-party technologies, permitting you to respond in real time to new fraud schemes. Fighting payment fraud is increasingly important as e-commerce sales continue in a growth mode. In fact, many experts predict that the current economy will result in even more fraud attempts and charge-backs, putting added pressure on retailers to keep fraud in check. You always have to be vigilant. However, there is no single technology—no silver bullet—that will detect fraud and keep your online payments secure.

The best course of action is to adopt a program that integrates all the elements of your prevention efforts, utilizes a combination of fraud-fighting tactics and filters, and leverages automation to the fullest possible extent. Your particular fraud controls and thresholds will depend on the nature of your business, merchandise, and your customers' buying habits. But no matter the size of your company or your product offering, you are likely to reduce your fraud losses through the deployment of a more comprehensive prevention approach.



Data Security

Never before has the retailer/customer relationship been so vital. With the growth of interactive social media and personal loyalty schemes, the retail industry is surging forward in terms of customer experience. Yet with competition so intense and consumers becoming ever more cautious, many retailers are unknowingly, and unnecessarily, putting this tenuous customer relationship into serious jeopardy.

The issue—data security. There have been plenty of news reports recently of major incidents where customer credit card data has been stolen from well-known retailers. These headlines about hacking and leaks should be ringing alarm bells for big businesses, but small and medium enterprises (SMEs) are often even more vulnerable.

All merchants need to take data security seriously. Careless handling of credit card details imperils the financial stability and customer base of any business. Yes, there are the obvious damaging financial consequences such as penalties, fines, and the cost of implementing improved security, but the ongoing loss of customer trust and the fear that

personal details have been leaked to criminals have more significant long-term consequences. The security of shoppers and their credit card details has been repeatedly shown to be a top concern. Consider that:

- A global survey found that 50 percent of consumers worry about credit card fraud (ACI Worldwide: Card Fraud Survey, March 2011)
- More than a third of consumers in the UK have experienced some form of card fraud (ACI Worldwide: Card Fraud Survey, March 2011)
- A survey of consumers in the UK found that 42 percent had been discouraged from making a purchase because they were worried about card fraud (Connected World: Card Fraud Survey, January 2011)

Banks, the credit card companies and retailers have all responded by taking steps to improve security. In the UK, for example, EMV (chip-and-PIN) cards were introduced to help reduce the risk of card fraud, but chip and PIN alone does not secure merchants. Even though the payment cards are more difficult to clone and copy, the card data is still susceptible to breaches while it's on a merchant's payment system. In an attempt to secure the whole environment in which the transaction takes place, the Payment Card Industry Data Security Standards (PCI DSS) were introduced in 2006 by the major credit card companies. These standards help ensure that a basic level of security is in place at merchant businesses to reduce the risk of card fraud.

By now, all merchants should be aware of PCI DSS, and many merchants that process, transmit or store credit card data are required to be PCI DSS-compliant.

In theory, with these new security standards the retail industry should be a safe haven for consumer data, with criminals forced to turn their attention elsewhere. Instead, a serious data breach happens every week on average and the number of hacking incidents seems only to be increasing. So what's going wrong?

For many merchants, PCI DSS compliance has become a bit like setting a house alarm, but using 1234 as an access code. The intention to protect against theft is there, but the execution is poor. Retailers just aren't giving enough attention to compliance. It's one thing just to fill out a self-assessment compliance form and tick the correct boxes, which on the surface indicates compliance, but it's another to keep up to date and be absolutely certain that a business is protected.

Small- and medium-sized businesses seldom consider themselves to be targets for card fraud criminals. But these businesses in particular must be warned: criminals do not only target big organizations. Larger companies are naturally richer targets; however, most have accompanying budgets and an IT department dedicated to protecting their vital customer information. Therefore, as PCI DSS regulations take hold, fraudsters are shifting their attention to 'softer', less well-defended targets like small businesses. In fact, nearly 96 percent of PCI DSS breaches take place with Level 3 and 4 merchants – typically smaller businesses that accept less than one million card transactions annually. Along with satellite branches of larger organizations, these are proven to be the most vulnerable organizations for attacks. According to research from Javelin (source), cybercrime in the U.S. targeted at SMEs totaled more than $8 billion in 2010.

It can be very difficult as a smaller organization to dedicate the time to ensuring proper and thorough PCI DSS compliance, but that doesn't mean there aren't options. Network management systems can be used to make PCI DSS compliance a simple, cost-effective and continual process with minimal fuss.

Nobody said compliance was easy, but compliance is not an option; it's essential. Retailers must begin to explore the opportunities, do what's best for the business, and avoid being next on the hacker's hit list.

Mobile, Mobile Everywhere, But What Does It All Mean?

Mobile payments, mobile commerce, and mobile POS are three commonly used terms today. Here, the various mobile methods are defined based on descriptions provided by MerchantWarehouse.com.

Mobile Payment. In its simplest definition, mobile payment is the payment for an item or service from or via a mobile device. While many today associate mobile payments primarily with "contactless" payments like near-field communication (NFC) or bar and QR codes, SMS, mobile web payments, and direct mobile billing are also included in its broader definition.

Mobile Payment Acceptance. Unlike the broader term of mobile payment, mobile payment acceptance signifies the ability to accept payments on a mobile device, whether it is a smartphone or tablet. The typical setup includes a free or low-cost attachment that allows for the swiping of traditional credit and debit cards. The device is connected, through the smartphone or tablet, to a credit- and debit-card processing application.

Mobile Commerce. While some interchange the terms mobile payment and mobile commerce, the latter has its own, distinctive definition. Mobile commerce encompasses mobile payment, but also includes a variety of mobile-based activities, including content purchase and delivery, money

transfer, auctions, browsing, marketing and advertising, and location based-services.

Mobile POS. Mobile point-of-sale (POS) is predicted to be the future standard, even among tier-one retailers. Many leaders are investing in mobile POS—hand-held checkout devices that serve as a payment extension to the company's larger POS system. While these new mobile POS devices have some of the same characteristics as mobile payment acceptance devices, they are much more robust in terms of features and reliability. These new devices will include the ability to accept mobile gift, NFC, QR/bar code, and include integrated loyalty and reward.

Tablet POS. In today's marketplace, more and more point-of-sale developers are focused on iPad and tablet development versus traditional systems. These new platforms afford developers with more options, more capabilities, and a lower-cost alternative, while retailers receive parallel benefits in terms of features and functionality, portability, and reduced cost. In fact, tablet-based POS systems open up a new opportunity for smaller retailers that, due to high cost, were not able to leverage POS in the past for their business.

With the growing number of mobile payment applications available to the consumer, associated challenges will also grow for retailers to accommodate the various forms of payments while remaining transparent to the customer experience.

As mobile payments continue to gain favor with consumers, the market is almost guaranteed to get more crowded with service provider options. Apple Pay, along with future Apple Watch applications, is purportedly the fastest-growing app for mobile payments. Samsung's recent acquisition of LoopPay is another reach into the mobile market through Android phones. And as recently reported by The Wall Street Journal, Google has shown renewed interest in Softcard, formerly called ISIS, the mobile payments company that was formed out of a consortium of AT&T, Verizon, and T-Mobile. There is also ConnectC, PayPal, and the Starbucks' approach with QR codes, to name a few additional options or potential options.

With the growing number of mobile payment applications available to the consumer, associated challenges will also grow for retailers to accommodate the various forms of payments while remaining transparent to the customer experience. There is a real possibility that a consumer might tap their device on a terminal in one store, use a QR code in another, and complete a transaction via a mobile application in another. There will be plenty of room for confusion from both the consumer and front-line employees at retail locations.

One More Consideration

In October 2015, the United States will begin the transition to EMV or chip-and-PIN or chip-and-signature technologies. This shift is being driven by the fact that the U.S. has emerged as the global capital for credit- and debit-card fraud, with a predicted $10 billion losses in 2015 alone. Chip-and-PIN technology reportedly provides more secure transactions particularly as it relates to card-present, in-store sales. The jury is still out on what its benefits will be as it relates to online transactions. When the technology was introduced in Europe, there were cases where online fraud rose as much as 150 percent.

The biggest change to retailers with the transition to chip-and-PIN card technology will be the assignment of liability from any fraudulent transactions taking place in stores. For retailers that do not upgrade their POS infrastructure to accommodate this new payment form, the liability would shift to the retailer from the card issuer as it has been in the past.

Most loss prevention executives have focused on theft as the biggest contributor to lost profits to their organizations as it can be measured in hard dollars. With the shift in liability, fraud will go from a balance sheet line item to a real drain on retailers' operations.

"Many retailers have not yet figured out how to handle this new way of thinking about fraud and its impact on their stores once the changes to credit and debit cards take effect, especially for those who cannot afford to immediately comply," said Joseph LaRocca, vice president and senior advisor on loss prevention for RetaiLPartners and formerly with the National Retail Federation. "The way we handle fraud incidents will change dramatically, not only from a liability standpoint, but also from the way those incidents will be processed through the legal system. Today card issuers can upload their cases in bulk, a process that is not yet in play for the retail community."

The Good News

Because widespread adoption of these new forms of payments is still in the early stages, there is the opportunity to plan accordingly.

Walgreens. The nation's largest drug retailing chain with over 8,000 locations, Walgreens has been accepting various types of mobile payments for several years. Walgreens' acceptance of NFC payments across the chain enabled its first adoption of Google Wallet and the expansion of Apple Pay. Since rolling out the new payment form, Walgreens has seen little to no impact on fraud levels.

The retailer credits its proactive approach to adopting new technology to a successful implementation. For mobile payments, that included a comprehensive communication strategy and partnering with key stakeholders within the organization as well as third-party providers, including its credit- and debit-card processor. Setting clear expectations and finding alignment and agreement at the start also helps the transition process to proceed more smoothly.

Walgreens' asset protection solutions team actively participates in weekly meetings with its IT partners so that any changes being considered or made to the POS systems take into consideration the need for proactive protection against fraud. These proactive measures are then designed into the back-end processes and are systematically included. The company also educates its front-end cashiers on how to handle mobile payments. The same basic principles apply to mobile payments as to traditional credit- and debit-card transactions—the card or the mobile phone must be present.

One of the challenges Walgreens faced in rolling out mobile payments was the misperception on the part of the field organization that fraud would be more prevalent. The company put together a comprehensive communication strategy to educate the field to help them overcome this misperception.

"The biggest challenge we faced was the misperception that the risk of fraud would be greater with mobile payments than with the traditional credit- and debit-card swipe," said Bill Inzeo, who is director of insights and intelligence and asset protection solutions for Walgreens. "We went to great lengths to educate our field organization that, if accepted according to policy, the risk factor does not go up with mobile payments."

When asked about the coming changes as it relates to EMV chip technology, Inzeo feels that the benefits far outweigh the challenges. Walgreens upgraded its POS systems a couple of years ago with an eye to future requirements. It made sure that all of its hardware was capable of accepting the new cards. They are now working with their programmers to develop code that will make accepting the new smart cards seamless to the customer and the associate.

"When it comes to adopting new technology like mobile payments or chip-and-PIN cards, you need to approach it from a business and financial perspective without the emotional ties to fraud and loss," said Inzeo. "We bring an objective point of view, evaluate the risk, and provide recommendations that protect our customers and the company, while delivering the shopping experience our customers and patients deserve and expect."

eBay. Online retail giant eBay has perhaps the most experience with mobile payments through its PayPal application. PayPal processed $46 billion in mobile payment volume in 2014, up 68 percent over 2013.

"Surprisingly, we have seen very little in the form of fraud attributed to mobile payments," stated Paul Jones, senior director of global asset protection for eBay and PayPal. "We attribute much of that to a well-thought-out and well-executed plan."

When asked what retailers should consider when entering the realm of mobile payments in their stores, Jones emphasized the need for structured agreements. Like his counterparts at Walgreens, he stresses the need for expectations to be set up front along with alignment and agreement on implementation. eBay offers its retail partners protection against fraud by assuming the risk and liability should a fraudulent transaction occur with its service. He urges others to address this point with their mobile payment service provider, whoever they may be.

Along with designing the interface for maximum ease-of-use for the consumer, retailers need to put network security at the forefront of the process. Echoing Walgreens' advice, Jones recommended that loss prevention teams need to be involved from the beginning of any new project that has the potential to disrupt business through loss or fraud. "You need to

be present from the start to be effective in the end," stated Jones.

Heinen's Grocery Stores. Regional supermarket chain Heinen's, based out of Cleveland, Ohio, currently accepts mobile payments in the form of Apple Pay and Google Wallet at its twenty-two retail locations. The company is also in the planning and implementation stages of converting its payment terminals to accommodate the new EMV CHIP technology.

According to John Guenther, director of risk management and information security for the merchant, the security challenges that exists between near-field communications (NCF) technologies like those found in mobile payment devices and EMV chip-and-PIN technologies are quite different.

"NFC devices concentrate on masking the consumer credit- and debit-card information from the retailer point-of-sale terminals through tokenization, while chip-and-PIN focuses on a more secure payment transaction by requiring a higher level of authenticating when using the card," explained Guenther. "Both forms of payment still have the potential to be breached—mobile payments through loading fraudulent cards into the device and chip-and-PIN for online transactions."

Not unlike other retailers who have transitioned to the new payment technologies, Guenther's advice is to develop a comprehensive plan and to be able to clearly articulate the goals and objectives behind making the proposed changes to the company's payment systems.

He recommends formalizing the project with a dedicated team, appointing a project manager to oversee all aspects of the conversion, engaging key stakeholders and third-party vendors, and asking the right questions from the start, such as:

- What middleware applications will be affected?
- What reporting functions will change and how?
- Will this be a standalone, integrated, or semi-integrated process?

These are just a few of the questions that will need to asked, answered, and understood for successful implementation.

"In the end, this journey into alterative payment forms is consumer driven and really not an option for most merchants if they want to continue to achieve a high level of customer service and satisfaction," said Guenther. "But along the way, it helped us create a heightened sense of awareness for PCI compliance and payment best practices for our organization."

Prepare for the Future

While the type of mobile payments that consumers will ultimately adopt and the number of options available to them will continue to grow, one thing is certain—mobile payments are here to stay and will only become more prevalent in the years to come. In order to remain competitive, retailers will need to find ways to accommodate mobile payments and provide a seamless shopping environment for their customers while accepting a whole host of mobile payments from a variety of devices.

"Retailers will need to follow the emerging mobile market closely so that they can deliver on consumer demands," concluded LaRocca. "At the end of the day, if a customer cannot conduct business in the manner that suits their individual needs, they will take their dollars elsewhere."

Preventing mobile payment fraud will take on a bigger role in the lives of many loss prevention executives with the upcoming shift in liability. But the good news in all of this is the fact that with proper planning, open dialogue with all key stakeholders, advancements in technology, and a comprehensive communication strategy, retailers are in a good position to meet the challenges head on.

Those who have already ventured into the world of mobile payments have so far seen little to no disruption to their businesses and feel that the goodwill generated among their customer base is well worth the time and efforts invested. "Technology in the retail environment is always changing," said Inzeo. "By being proactive, you can adjust to anything. If you are involved from the beginning of the process, you can find success."

Contributors to this free report include Chris Trlica, Bill Farmer, Scott Richard, JD Sherry, Lee A. Pernice, and the Association of Certified Fraud Examiners.