BRIDGEFORCE®

Turning risk into opportunity℠

SPECIAL REPORT

Combating Fraud and Data Breaches

End-to-end strategic management insights

Overview

In 2014, the number of data breaches increased nearly 28%, according to the Identity Theft Research Center (IRTC). The 2014 increase was on top of an 18% increase in 2013. The shocking truth is that more than 675 million data records, according to ITRC estimates, were compromised last year.

In recent months, news headlines have been filled with warnings for consumers regarding credit and debit card fraud. The most notable were the Target, Neiman Marcus, and Home Depot store compromises. It was estimated that over 160 million consumers had sensitive data compromised after shopping at the three retailers. Neiman Marcus disclosed that their breach occurred for several months ranging from July to October 2013, while Target was compromised in late November to mid December 2013, in the midst of the holiday shopping frenzy. Home Depot was compromised between April and September of 2014. These types of compromises not only impact large retailers like Target or Neiman Marcus from a reputational perspective, but also deeply impact financial institutions large and small.

In this report, we outline the most common ways consumers are compromised and the impacts of fraud on consumers, merchants and financial institutions. Fraud organizations have become increasingly sophisticated in their means of obtaining credit and debit card data. The days of obtaining credit card information from stolen wallets and mail are gone. Today's thieves leverage the ever-evolving world of technology and the increased usage of credit and debit cards.

How is data stolen in large quantities?

In today's data-rich world, almost everything a consumer does can be tracked. It can be daunting to protect oneself from being a victim of fraud. Below are common ways data is stolen in large quantities:

1. Malware placed into merchant POS platforms

This type of data gathering is on the rise and designed to integrate into the POS (i.e. cash registers) to monitor credit and debit card authorizations. The BlackPOS malware, as it is known, is designed to gather the decrypted card information that exists for a brief time during the transaction process, store it, and transmit it to a space where the criminals can obtain it. This type of attack is what has been identified by both the security firm ISight and the U.S. Secret Service as the method behind the Target compromise.

2. Merchant POS terminal tampering

This type of attack can come in different ways:

   a. Skimming devices
      Skimming devices can be placed on the outside or inside of the POS device, allowing for capture of mag stripe data and/or PINS within the terminal. Data is then stored within the device until the attacker comes back to retrieve it or until it is transmitted remotely to a data gathering source.

   b. POS terminal swap out
      Attackers infiltrate the POS terminals directly and swap them out with their terminals that are capable of gathering and storing card data.

3. Payment processor data breach

Multiple merchants can be impacted at the same time with this type of attack. This is one of the more difficult situations for financial institutions to identify within their fraud monitoring because of the range of merchants where the data is gathered. For banks, identifying this type of breach when examining recent fraud claims is very difficult due to the variety of merchant types that could be using the same processor.

Consequences and impacts

Consequences of such large data breaches can be far reaching. They impact everyone involved in the process: the consumer, merchant, and bank that issued the credit or debit card.

Customers have all the power when it comes to bank and merchant recovery after an attack.

1. Consumer

Although the consumer is often the least impacted from a long-term financial perspective because most issuers have zero liability fraud protection, they are the ones that impact future consequences for merchants and banks. If consumers do not feel that their bank or a merchant is doing their best to protect them as customers, they could change their spending habits. This could include using more cash, changing credit cards, or even in the most severe instances, not using the merchant at all. Customers have all the power when it comes to bank and merchant recovery plans after being attacked. The news media is a powerful influence in shaping consumers perspectives and reactions following a large breach.

2. Merchant

Merchants typically bear as much or more of the blame in consumers' eyes following a breach as the banks do, depending on how and where the breach occurred. The impacts can be short-lived or long-lasting. Consumers expect large merchants to have good controls in place to prevent such breaches discussed in this report. Consumer distrust is the largest enemy for merchants following a breach that occurred within their walls. The negative media attention following a large attack can impact a merchant financially in the form of reduced consumer spending, fraud losses, and legal fees. Overall reputational damage is also a major concern.

3. Financial institutions

Banks also experience large impacts when major breaches occur. These come in the form of fraud losses, operational expense increases, and reputational damage. The increased fraud losses will vary based on the type of data breach and information stolen. If the subsequent fraud is more of online activity, they will have increased charge back rights, but if it is aimed at point of sale purchasing, the impact can be severe. Beyond financial consequences, the bank also is at risk for reputational damage, even if the breach was clearly not within their walls.

Resolution procedures

With the sophistication of attackers in today's world, prevention is more difficult to accomplish. Remediation is something everyone needs to be prepared to implement. It is not a matter of if an attack will happen; it is a matter of when the attack will happen.

1. Consumer

Consumers want to have confidence that their bank will protect them. Upon learning of a breach, consumers need to closely monitor their card activity, looking for suspicious transactions via the monthly billing statements and online via the bank's website. The first thing consumers should do upon detecting fraud on their account is contact their bank. They should request that the current account be closed and a new card with a new account number and CVV be issued.

Additionally, consumers should leverage the technical capabilities that many financial institutions' online banking platforms offer. Most platforms allow consumers to sign up and customize alerts on their accounts. These alerts can be leveraged many ways, the most popular being email or text. This is a great way for consumers to monitor their own card activity and be aware of suspicious charges. The alerts allow the customer to define what they feel is suspicious to them, (e.g., international transactions, or charges greater than $300). It serves as a valuable complement to what the bank provides and allows for much earlier detection than simply reviewing their billing statement each month.

Another emerging trend that has become available for consumers to leverage is free credit score monitoring. More and more financial institutions are offering a monthly credit score feature on some of their products. These features range from just displaying the score, to showing additional attributes that impact the score as well. This can be another valuable tool for consumers to self-monitor credit health and keep vigilant against allowing fraud on their account. Drastic changes in score or increased inquiries that the consumer isn't familiar with, are both indicators that account(s) or identity may have been compromised.

2. Merchant

If the attack happens at the merchant, they need to take responsibility and quickly address the issue with vigor and conviction to calm consumer concern and protect reputational damage. This includes complete cooperation with the issuers, banks, and government agencies that may be involved in investigating and fixing the issue.

3. Financial institutions

Banks are often the first point of contact when consumers are impacted or are worried about being impacted. After a large breach is made public, the bank needs to be prepared for the operational impacts that will occur.

By the time a breach is made public, the fraud has been occurring for some time.

Call centers will experience increased call volume with customers requesting new cards due to fraud or as a precaution. They are also going to have to field questions and concerns about the breach itself. Banks should be prepared to quickly draft and publish talking points for their associates to use during these types of customer interactions. Confident messaging from associates is crucial for maintaining consumer confidence and trust for their bank.

Pro-active customer outreach is another way banks can assist in controlling messaging regarding breaches to their customers. This method allows the bank to clearly inform the customer what the bank is doing to protect them and what steps the customer needs to take as well. The recommended channels for this type of communication are IVR messages, email, text, or mobile app notifications.

Fraud Strategy Teams need to immediately begin analyzing recent claims data to identify trends related to the breach. This includes leveraging data across different products. For instance, if a customer's credit card account has been compromised, there should be enhanced monitoring of their debit card to look for similar activity. Most likely, by the time the breach is made public, the fraud has already been occurring for some time. In addition, accounts that are confirmed as being part of the breach population need to be closed down and new plastics with new account numbers should be issued to the customers. It is good practice to monitor any populations of accounts that are confirmed as being breached, but also those suspected of being breached. This will allow swift reaction if those accounts begin to experience higher than normal fraud levels. Remediation actions need to be carefully balanced between limiting fraud losses and causing negative customer experiences.

Detection and prevention opportunities

1. Consumer

Consumers do not have the ability to protect themselves from their information being stolen via the types of large breaches discussed in this report. They rely on merchants and banks to protect them.

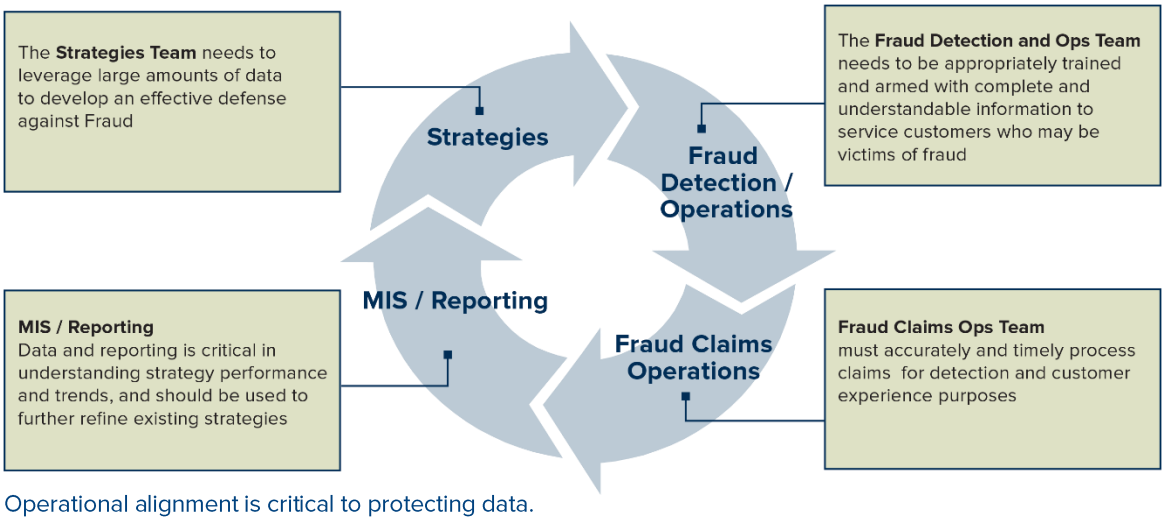
2. Merchant

Merchants play a key role in the prevention of these types of breaches. It is the merchant's responsibility to ensure they are using every means possible to safeguard consumer data. That means leveraging complicated encryption and sophisticated security processes and procedures around the handling of transaction level processes. This also extends to any data warehouses that may store consumer information. Other ways merchants can help themselves and customers, is to leverage technology that interrogates devices using their websites. There are solutions available that allow merchants to monitor IP addresses and devices that are entering their websites. The solutions can identify known "bad" devices or IP addresses and alert the merchant so that the proper fraud decisions can be made.

3. Financial institutions

At the financial institution level, prevention of a data breach is similar to that of the merchant. Banks not only need to protect themselves from a breach happening to them directly, but also have the responsibility of preventing impacts to their customers and shareholders.

The key to controlling fraud losses within financial institutions is detection. In order to maintain the highest level of detection, a bank needs to have its strategies and operations teams in lockstep with each other. The strategies team also needs to ensure that multiple types of data are used in making the most intelligent decisions if they are going to properly balance fighting fraud and having a best in class customer experience. Below are key components that must work together to form a solid Fraud Detection Model.



Operational alignment is critical to protecting data.

a. Strategies

The Strategies team needs to be able to leverage large amounts of data and combine them together in order to develop the most effective defense against fraud. This group is ultimately going to be the one that controls the customer experience. Customers may be impacted at the point of sale and also in card re-issue.

i. Point of sale strategies

These strategies focus on customer interactions at the point of sale. Customers' transactions may be declined, approved, or referred and queued for a fraud associate review. It is a critical part of any bank's customer experience perception. Business leaders must agree on false positives that meet the expectations of both shareholders and customers. Daily fraud claims data must be combined with daily authorizations data to identify the active trends and also be more pro-active in making decisions on transactions that are associated with accounts that may have been compromised. Fraud flagging or tagging is the most effective way to identify these accounts within authorization strategy treatment. Other ways to leverage strategy logic is to incorporate geo-variance calculations into your card present strategies. This, along with fraud model scores, can help identify many fraud transactions.

ii. Mass compromise / point of compromise (POC) strategies

These strategies leverage information directly from issuers like Visa and MasterCard and also from internal processes. The most effective way to monitor this type of activity is to have a reporting database that you can load potentially compromised accounts into and monitor their confirmed fraud rates over time. This will help prioritize block and re-issue actions as most banks need to manage plastic expense as well as customer experience.

In addition to identifying mass compromises, the team should focus on daily processes that help identify smaller compromises that could be from skimming or small data processing breaches. This serves to complement any mass compromise block and re-issue strategies.

Whether you address both large and small breaches, or just target large ones, it is a best practice to flag or code all the accounts that you suspect could be compromised if you have not already re-issued them. Typically, you could then use this within your point of sale treatments to help mitigate losses.

iii. Leverage technology solutions

There are many solutions available to financial institutions to assist in detection of fraudulent transactions. The ones that are most valuable against transaction level fraud are scoring models and decision engines that incorporate geo-variance, and known "bad" merchant profiles. In addition, some solutions are able to identify devices that are known "bad" or appear to be fraudulent merchants.

b. Fraud detection / servicing operations

Whether your institution leverages associates for both detection and servicing or just servicing, it is critical that proper capacity planning, load levels and associate talent are in place. It is also necessary to have swift and accurate information flowing to customer facing associates on any breach or fraud related topics that are in the media. They need to be armed with good, accurate, and easy to understand information to be prepared and appear confident when customers ask them about what they have read or seen in the news. If the customers do not feel confident in the bank representatives that they speak with, their confidence in the bank overall could suffer.

c. Fraud claims operations

Accurate and timely processing of claims is crucial for detection purposes and for customer experience. Customers need to see timely and accurate processing of their claims as this is a sensitive time for them and the bank has assured them in most cases of zero liability for fraud charges to their accounts. If possible, claims systems should be able to archive each transaction that was deemed fraud in a data warehouse for later use in reporting and data analysis. Transaction level fraud data is critical for understanding performance of existing strategies and for development of new ones.

d. MIS / reporting

Fraud reporting is critical to being able to understand strategy performance, current and past trends, and customer point of sale experience. Fraud organizations need robust reporting if they want to be able to effectively manage the fraud life cycle and address trends in a fluid manner.

Conclusion

From a fraud and breach perspective, there are many interdependencies required to create a successful program. Careful attention to and coordination of each element is critical from processing, detection, rectifying and identifying claims as well as the overall customer experience. Without thoughtful, strategic, operational planning an organization could experience deep reputational damage.

How Bridgeforce can help

Bridgeforce has the skills and resources available to assist you with refining or developing internal processes and procedures for managing large data breach attacks. Our experienced, industry proven leaders have helped several of the largest banks proactively identify key concerns and have worked with them to close gaps related to reducing fraud losses. We invite you to reach out to us to discuss this report and any help your team may need to achieve your fraud detection and mitigation objectives.

Contact us for more information

We would be happy to talk freely about our experiences in this area and help you understand where our services would be most valuable.

Brian Reiss, President
Phone: +1 212.245.6769; breiss@bridgeforce.com

Cris Bennighoff, Senior Program Manager
Phone: +1 302.598.9308; cbennighoff@bridgeforce.com

David Sanders, Senior Program Manager
Phone: +1 302.932.7692 dmsanders@bridgeforce.com

About Bridgeforce

Bridgeforce, a specialized multi-national consulting firm, has been solving complex problems for companies involved in consumer and/or small business lending and payments for nearly 15 years.

Over 75 percent of Bridgeforce consultants come directly from client-side leadership positions across multiple parts of the credit lifecycle. Combined with subject matter expertise in operations, technology, strategy and regulatory issues, Bridgeforce brings a deep and practiced understanding of the lending and payment environment to each new client.

With market, regulatory and technological changes continually altering the risk landscape faced by sophisticated lenders, corresponding business changes require hard choices and the courage to make them. Bridgeforce has a strong record of helping clients make these choices by providing best-fit solutions that are achievable and provide meaningful change for each client.

The company operates in several regions with core markets and offices in the US and UK and additional operations in the Euro zone, North America and Latin America. The close working relationships between Bridgeforce with the US and European banks gives the company valuable insight into the interconnected regulatory movement and strategic trends across countries.

Bridgeforce success can be attributed to a culture of collaboration, support and trust fostering innovation, thought leadership and evolving best practices recognized within the industry.

Bridgeforce Inc.
US: 101 Ponds Edge Drive, Suite 100 ■ Chadds Ford, PA 19317-8301
Phone: +1 610.228.4508 ■ Fax: +1 484.770.8259
bridgeforce.com

BRIDGEFORCE®
Turning risk into opportunity℠