



JAVELIN STRATEGY & RESEARCH

Consumer Survey on Data Breach Notification

Conducted by
Javelin Strategy & Research
June 2008

Executive Summary

With data breaches continuing to make daily headlines, consumer awareness of identity theft and the security of their personal information will only be heightened. Publicity of large-scale breaches has caused an outrage among consumer advocacy groups as well as adversely affected organizations such as banks and issuers. Some incidents have led breached institutions to be stricken with class-action lawsuits, as was the case with TJX and more recently with the Hannaford breach.

Above any financial losses, however, is the breached institution's reputation, which is heavily dependent on the company's image, brand and its relationships with customers. While data breaches can cost tens of millions of dollars to repair because of fines, security upgrades and notification efforts, reputation is one asset that may not be guaranteed as fully restorable.

Key findings from a survey of breach victims highlight the implications that security breaches hold, in terms of consumers' expectations regarding the breached institution, financial behavior and perceptions of identity fraud:

- For 40% of consumers, security breaches changed their relationships with the affected institution or business.
- 55% of breach victims offered a fraud protection solution were satisfied with the institution's handling of the incident, almost double the 31% of those who were satisfied without being offered any kind of restitution.
- The majority of breach victims (56%) prefer a solution that prevents fraudulent use of their information, rather than detecting or resolving fraud after it has occurred.
- Confidence and buyer behavior are severely impacted by security breaches, with 55% of victims trusting the affected organization less, and 30% choosing to never purchase goods or services again from that organization. As a result, breached institutions must go beyond basic notification and take assertive action to mitigate the risk placed on victims.
- Breach victims are beginning to expect fraud protection assistance from the institution, with 36% already having been offered some kind of identity fraud protection service.

Methodology

Data was collected and analyzed in May 2008 via an online consumer survey of 400 data breach victims. In addition, Javelin conducted in-depth interviews with two breached institutions who had recently implemented a fraud protection solution for affected customers. The result of this project is a strategic assessment of how breached institutions should respond to data leakage incidents involving highly sensitive information, and the solutions that should be offered to victimized customers and/or employees.

An Era of Data Insecurity

Introduction

Safeguarding customer data is a basic component of good business practice, yet the number of compromised accounts due to security breaches is at an all time high. Since January 2005, nearly 227 million¹ records containing sensitive information have been exposed through security breaches, and over 35 million² Americans have had their information compromised in a data breach.

There have been more than 1,000 reported data leakage incidents since 2003.³ Data security has come under increasing scrutiny as breach incidents continue to make news headlines on a frequent basis. An environment of mistrust is becoming more entrenched among consumers, and the media's preoccupation with sensationalizing data breaches only adds fuel to the fire.

The infamous TJX and U.S. Department of Veterans Affairs breaches single-handedly placed data security as a prominent fixture in the media spotlight, even going as far as to prompt legislative action. After suffering the loss of 94 million records comprising credit and debit card numbers, as well as 455,000 addresses and social security numbers,⁴ TJX has spent or placed in reserve more than \$256 million to repair the damage. The disclosures sparked widespread concern over the perceived lack of information security controls, prompting a sweeping overhaul of information technology (IT) development, operations and maintenance organization, as well as top-level personnel changes.

As Breach Notifications Proliferate, Consumers Begin to Question the Safety of their Data

Data breaches are defined as names matched with social security numbers, driver's license or state identification numbers; or account numbers or credit or debit card numbers with passwords or codes. Thus far, 41 states have legislated differing versions of data breach notification bills, creating a patchwork of laws that makes compliance all the more complicated.



¹ Privacyrights.org, accessed May 14, 2008.

² Javelin Strategy & Research, 2008.

³ Etiolated.org, accessed May 14, 2008.

⁴ According to court documents filed Oct. 23, 2007 in Massachusetts by bank associations. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>, accessed 11/05/07.

An Era of Data Insecurity

California's law SB 1386—the first notification law to go into effect on July 1, 2003—requires automatic notification whenever private data has been breached—unless the data is encrypted. More than five years after this law was enacted, not all states have followed suit. Among the 41 states that have enacted some sort of breach disclosure law, most follow the basic tenets of California's original law: companies must immediately disclose a data breach to customers, usually in writing. In California, there is a private right of action, and there are very few exemptions. Laws in other states may allow more exemptions or do not allow a private right of action. The Massachusetts law pertains to paper record as well as computer data.

The original legislation was important to alert businesses and consumers to the hazards posed by under-protected electronic data. Organizations' indiscriminate exposure of customer and/or employee data may be sending the message to consumers that institutions cannot be trusted to correct lax security. Data breach legislation has been instrumental in exposing the flaws in current systems and in improving the protection of consumers. Ultimately, it is up to the breached organization to correctly assess the risk to the victims and adequately address consumer security concerns and determine which solution is appropriate for their consumers. Mandated reporting of data breaches has dramatically elevated consumer awareness of data protection and potential for identity fraud to ensue as a result.

Security Breaches Diminish Consumer Confidence and Weaken Buyer Behavior

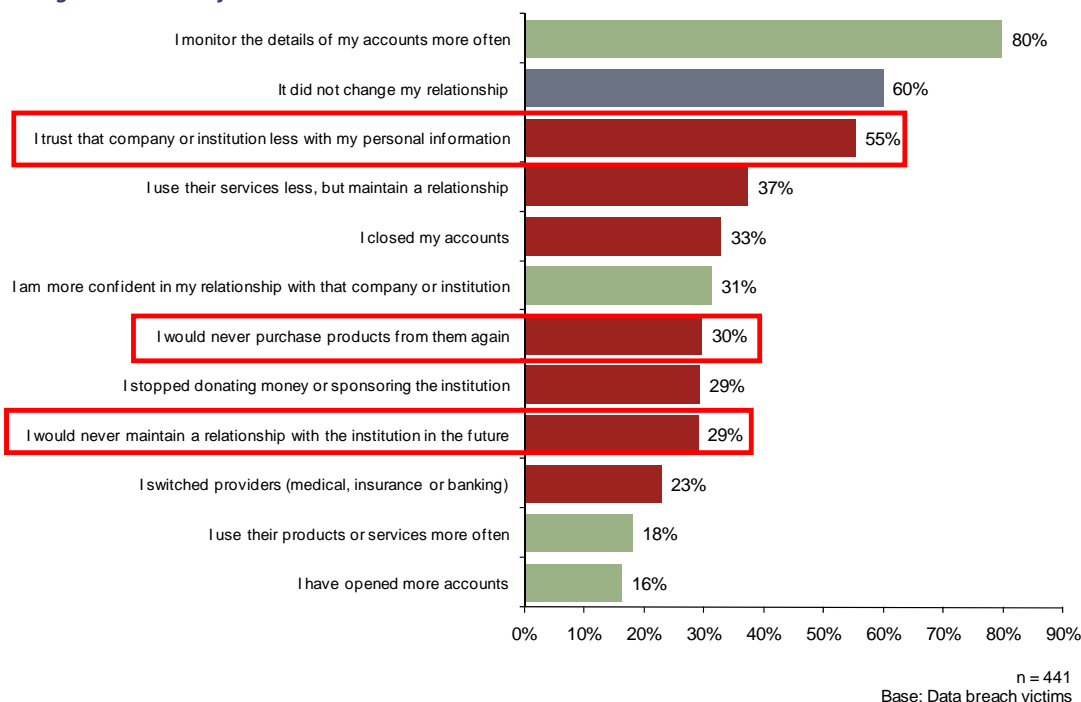
Overall, most reactions that breach victims exhibit are generally harmful to the institution’s business, resulting in fewer transactions and weakened customer loyalty. As a result, it is crucial for a breached institution to effectively alleviate the sensitivity that consumers may experience in response to notification, through straightforward explanation and offering assistance to protection.

When data breaches occur, victims can react strongly and disapprovingly, as evidenced by the data presented below. Customer trust is severely impacted by data loss incidents, with 55% of breach victims expressing diminished confidence in the breached organization’s ability to protect and manage their personal data. This decrease in trust has serious implications for a company’s brand, reputation, customer relationships and overall business.

Breach victims are expressing that they are ready to react decisively with their wallets if their private data is compromised. Thirty-seven percent of victims state that although they are continuing to maintain a relationship with the institution, they use its services less, while 30% of victims state they would never purchase from the breached business again. Furthermore, 29% expressed they would not maintain a relationship with the institution in the future.

How Victims Respond to Data Breaches

We’d like to know how your relationship with the company or institution changed as a result of the data breach.



Security Breaches Diminish Consumer Confidence and Weaken Buyer Behavior

Breach Victims' Perceived Likelihood of Identity Theft

- 27% of breached consumers reported they were more likely to be victimized by identity theft
- 12% of breached consumers reported they were much more likely to be victimized by identity theft

Nearly 40% consumers believe they are more prone to identity theft because of a data breach.

Notification of a data breach is likely to cause confusion and even fear among those informed. Given the tremendous misunderstanding surrounding identity theft, identity fraud, and security breaches, there will also be those consumers who may mistakenly deduce that the exposure of their personal information inevitably has resulted in actual fraud.

Among those individuals who have had their data breached but not yet misused, four out of ten consumers believe they are in significantly greater danger of falling victim to identity fraud and anticipate enhanced vulnerability. Clearly, consumers' perception of security is strongly affected by their discernment of data breaches and the effect felt by receiving notification.

Institutions Must Purchase Protection to Secure Customer Trust

While data breach notifications are seen by most customers as evidence of ethical and legal responsibility, consumers are now beginning to question what is being done to repair the damage that has occurred. The good news is that institutions are becoming more thorough with notification as a best practice, which aligns with consumers' desire to be informed clearly and in a timely manner.

However, while notification allows the consumer to take protective action and to monitor their accounts more closely, from a customer service perspective, it is to the advantage of the institution to be proactive and offer assistance on behalf of the customer, especially if the exposed data is highly sensitive. Breach victims should not be obliged to ask for help in protecting their identities when the fault of the breach lies with the institution. It is the responsibility of a breached organization to go beyond basic notification and offer a *solution* to the problem, not just an apology.

Providing a fraud protection solution is an effective way to address those breach victims that may react strongly to notification. In doing so, the institution is showing that it is assuming full responsibility for the problem by offering an appropriate solution to safeguard customers against potential fraud. Implementing fraud protection services is a straightforward process, nevertheless institutions are continuing to follow the letter of the law and three out of ten breach victims are stating that their institution took no action beyond notification.

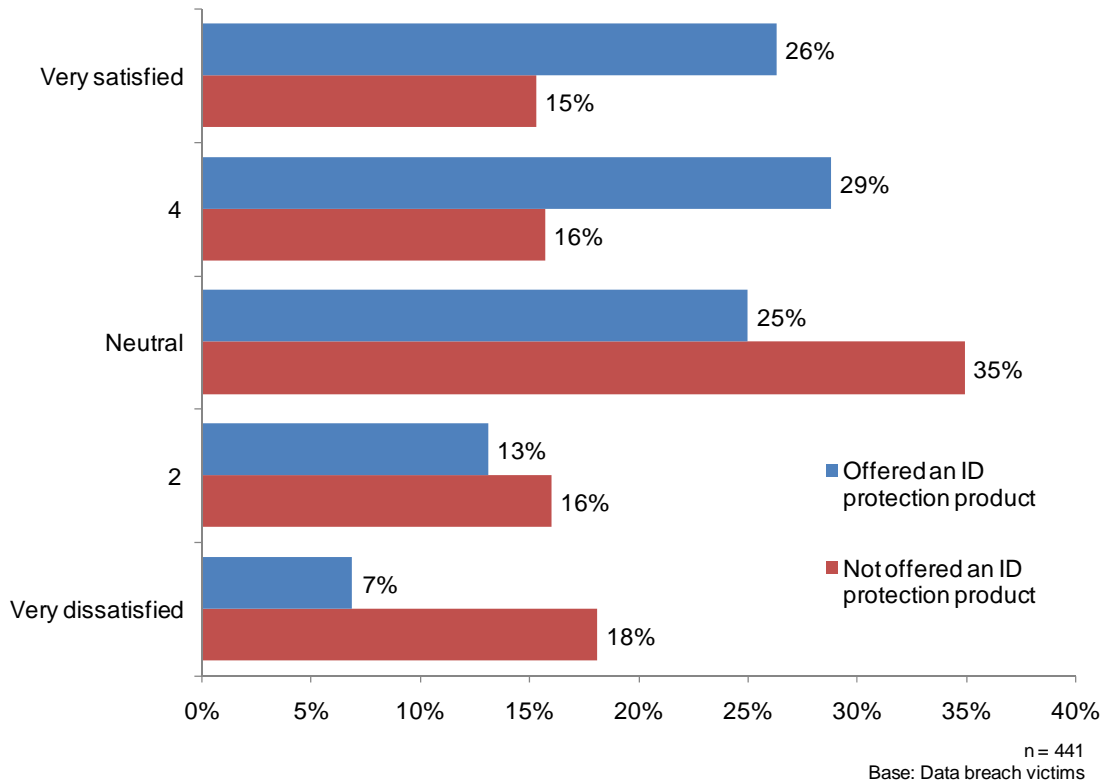
Significantly Higher Satisfaction among Breach Victims Provided with a Fraud Protection Solution

Providing a fraud protection solution makes a tremendous difference in customer approval of the breached organization’s management and handling of the incident. There is a marked disparity in satisfaction between breach victims that were offered a discounted or complimentary fraud protection service and those who were not.

More than half of breached consumers were satisfied or very satisfied with the manner in which the organization handled the breach, compared to 31% who were not offered any fraud protection solution.

Breach Victims’ Satisfaction with Institution’s Response

Considering the company that reported the data breach, how satisfied are you with their performance handling the data breach?



Data Breach Victims Resoundingly Favor a Solution that *Prevents* Fraud

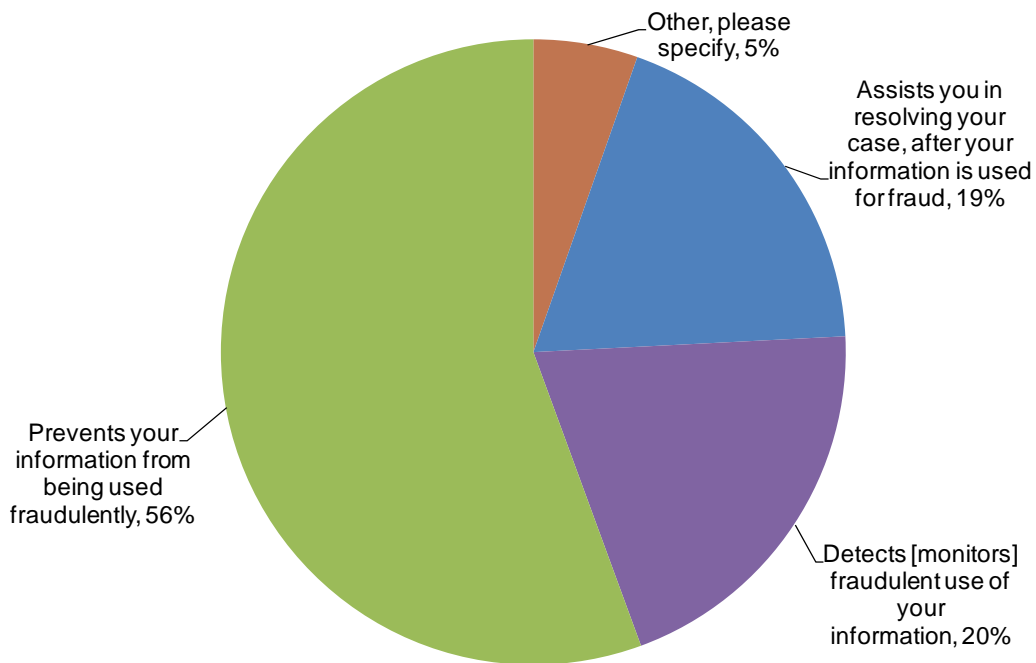
Data breach victims demonstrate an overwhelming preference for a solution that prevents their information from being used fraudulently, over those that detect or resolve fraud after it has occurred.

This is an obvious choice because the very nature of prevention poses the greatest impact in mitigating fraud, averting both costs to the victim and institution (and consequently any time or effort involved in reporting detected fraud and resolving it). Fraud protection solutions that provide prevention present less worry and maintenance for the consumer, and proffer the most powerful protection against actual misuse.

Prevention is especially crucial in the case of new accounts fraud, which is perpetrated with the use of stolen social security numbers and represents the most difficult type of fraud in terms of discovery and resolution.

Breached Consumers' Preferences for Fraud Protection Solutions

If a company or institution that experienced a data breach of your personal information offered you an identity protection service, would you most prefer a service that...



n = 441
Base: Data breach victims

Data Breach Victims Resoundingly Favor a Solution that *Prevents* Fraud

Fraudulent new accounts such as credit cards, loans, telephone accounts can go undetected for longer periods, with victims not only incurring greater financial losses but undergoing tremendous emotional stress in spending months and potentially even years repairing the damage done to their good name.

Consumers want prevention tools (56%) and early last year many prevention tools entered into the market space. The industry typically provides detection tools rather than prevention to breach victims, even though only 20% consumers prefer a detection-oriented solution.

There are several preventative solutions out in the market, with each offering varying services and features. The ideal preventative solution would be one in which the vendor plays an active role in contacting the consumer for authorization to open a new account, by acting as the notifying entity to the consumer. This has the effect of providing a means to track criminal attempts to create fraudulent accounts, as well as respecting the consumer's privacy by keeping their phone number confidential. The audit trail is also highly useful in assisting law enforcement in investigating fraud cases, which can be leveraged by those individuals who may decide to press charges.

The ideal preventative solution would also involve a phone call to the individual. For this to work, multiple numbers should be provided (cell phone, home phone, or work), and there must be a guaranteed way for the user to identify the source of the call as legitimate.

Responding to a Security Breach: What Should the Institution Offer to Victims?

When data breaches do occur, the circumstances of the theft and the types of data stolen should guide the actions offered to breach victims. The affected organization must go back and evaluate the various types of data stolen and the risk of fraud. Breaches that are targeted specifically to obtain private data are clearly more serious than breaches where the information is obtained incidentally. The specifics of which identity fraud protection services to offer depends on the sensitivity of the type of data that has been compromised. Furthermore, institutions should engage in a structured, analytic process of evaluating the precise types of services to offer, based upon the variables of the breach.

Consumer-Facing Breach Evaluation: Data, Threats, Fraud Solutions, Resolution

Data	Social Security Number (SSN)	Credit or Debit Card Number	User ID and Password	Checking Account Information	Minors
Consumer Threats	New accounts fraud	Fraudulent charges	Account Takeover	Check fraud	New Accounts & Utility Fraud
Consumer Fraud Solutions	Preventative Solutions	Electronic monitoring; financial account alerts	Account alerts; change password	Monitor checking account; account alerts	Monitor credit headers and utility records
Resolution	Identity theft insurance, Restoration services	Block/reissue credit or debit cards	Close account	Change account number	Insurance and restoration services

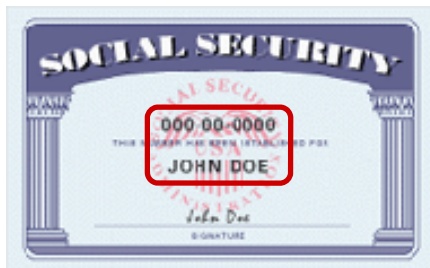
When social security numbers are among the types of data that have been breached, it is becoming the industry standard for institutions to offer complimentary fraud protection assistance for at least one year. In the case of breached financial information such as account numbers or payment card data, banks and card issuers closely monitor financial accounts on the back-end, blocking and reissuing accounts based on the risk. Consumers can also monitor checking or credit card accounts on their own, through opt-in email alerts.

Breached institutions are increasingly offering complimentary one-year credit monitoring or preventative solutions to victims with exposed social security numbers or other highly sensitive data, given that it is the single most valuable piece of data used to identify an individual. More than one-third of all breach victims surveyed have been presented with an option to enroll in some kind of identity fraud protection solution.

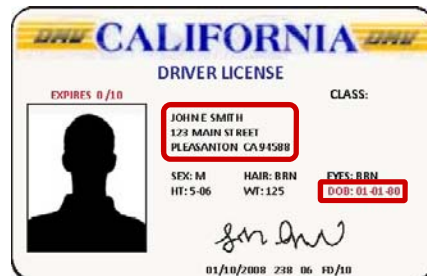
Responding to a Security Breach: What Should the Institution Offer to Victims?

To provide greater convenience for breach victims with the maximum amount of protection against new accounts fraud, institutions would fare best by offering a robust, *preventative* fraud protection solution. Vendor-provided preventative services prompt issuers of credit to reasonably and accurately verify the identity of the credit applicant, thereby impeding the creation of potentially fraudulent new accounts.

Sensitive information: Name and social security number
Threat: New accounts fraud



Sensitive information: Name, address, date of birth, driver's license number
Threat: Fraudulent new driver's license; new accounts fraud



Optimal Solutions: Fraud Prevention

Sensitive information: Name, address, date of birth, social security number
Threat: New accounts fraud

WIAA
WISCONSIN INDEPENDENT ATHLETIC ASSOCIATION

MEDICAL EMERGENCY AUTHORIZATION FORM
TO BE COMPLETED BY PARENT AND RETURNED TO SCHOOL PRINCIPAL'S OFFICE

Name of Student Athlete _____

As Parent or Legal Guardian, I authorize the team physician or, in his absence, a qualified physician to examine the above-named student and, in the event of injury to administer emergency care and to arrange for any consultation by a specialist, including a surgeon, he deems necessary to insure proper care of any injury. Every effort will be made to contact parent or guardian to explain the nature of the problem prior to any involved treatment.

Name _____ Date _____
(Signature of Parent or Guardian)

Parent's Home Phone _____ Business Phone _____
Emergency Contact Person
Name _____ Phone _____

Social Security _____
Address _____

FOR SCHOOL USE ONLY:

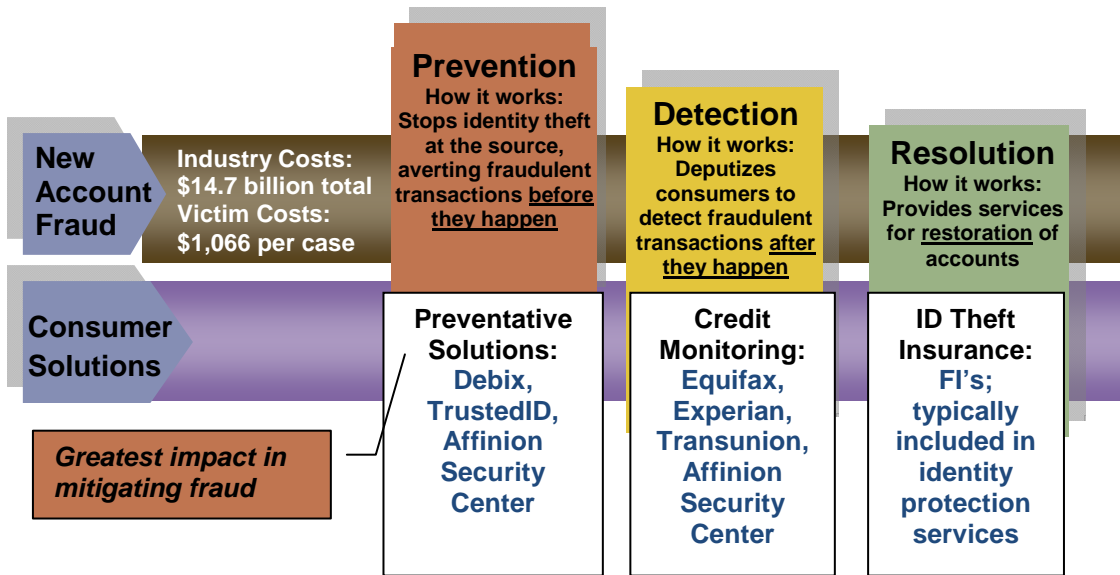
Completed Form Received _____ Date _____ Name _____
Duplicate Copy Distributed to _____
Date _____
Insurance coverage by parents Yes _____ No _____ Unknown _____
One copy filed in Student Permanent Record By _____ Name _____
Date _____

Prevention, Detection and Resolution

The Javelin Prevention, Detection and Resolution™ Model depicts a three-pronged approach to fighting identity fraud, an ever-evolving crime that involves multiple channels, methods and techniques.

Prevention poses the greatest influence in mitigating potential financial and reputation-related harm to a breached institution, minimizing any impact to the consumer. Detection and Resolution, however, occur after the fact; fraud has already occurred and efforts to make the victim whole again can be costly, time-consuming, and in a worst-case scenario, too late. In the case of a merchant breach, the victim may decide to end the relationship with the business.

Javelin Prevention, Detection, and Resolution™ Model



56% of data breach victims prefer a fraud prevention solution, 20% favor detection and 19% choose resolution

Prevention, Detection and Resolution

Prevention: The Strongest Weapon against Fraud

Fraud alerts services are designed to proactively prevent new accounts fraud, by requesting lenders to verify an applicant's identity before issuing credit. The strategic advantage of fraud alerts lies in the ability to prevent new accounts fraud before it occurs, gives fraud alerts a lead over detection-oriented services.

While there are several preventative solution vendors in the consumer identity protection space, the Debix Identity Protection Network is unique because it is the only vendor to play an active role in the new accounts fraud prevention process. This allows the Debix Identity Protection Network to actually prove which new accounts are valid and which are fraudulent. Rather than prompting lenders to verify the credit application directly with the consumer, the Debix Identity Protection Network request that creditors first contact Debix, which in turn alerts the users via its automated system, thereby allowing the user to immediately authorize or deny the credit application.

Therefore, the Debix Identity Protection Network can track actual attempts at fraud, as well as secure valid new accounts. From October 2007 to March 2008, Debix Identity Protection Network customers responded to over 68,000 Instant Authorization™ requests and stopped over 850 reported attacks. More recently, Debix is leveraging its Identity Protection Network to engage with law enforcement to pursue criminals that have attempted to perpetrate new accounts fraud.

Furthermore, Debix Identity Protection Network customers are ensured that the Instant Authorization call is legitimate because of their own pre-recorded voice message, which will be played any time they receive a call. The pre-registered phone number and unique PIN add yet another layer of security by ensuring that the right person can accept or deny the application for credit. In addition, the Identity Protection Network locates customers by using up to three phone numbers (thereby enhancing access to the customer), while allowing customer privacy to be maintained by keeping the numbers confidential.

What about Credit Monitoring?

Unlike preventative solutions, credit monitoring does not prevent identity theft and is designed to inform the user of potential fraud after it has occurred. Currently, only 16% of consumers view their credit reports as part of a credit monitoring service.⁵ Credit monitoring is offered by vendors such as Affinion Security Center and the three credit bureaus (Equifax, Experian and Transunion). Prevention and detection solutions (in the form of fraud alerts services and credit monitoring, respectively) can be purchased from Affinion Security Center .

⁵ 2007 Annual Household Finance Survey, Javelin Strategy & Research, 2008.

Prevention, Detection and Resolution

It is important to note that a complete credit monitoring subscription will include access and monitoring of reports from *all* three credit bureaus, not just one. When a data breach occurs and the affected company only purchases single-bureau reports for victims, full protection is not being provided. The three credit bureaus do not share data, and a single-bureau report presents an incomplete representation of the individual's credit history.

Resolution Services

Resolution services, which usually come in the form of insurance, are designed to provide services and tools for the restoration of accounts and creditworthiness. Identity theft insurance coverage varies among different fraud protection providers. Some insurance reimburses victims for out-of-pocket expenses such as lost wages and legal fees, but not necessarily the entire cost of actual losses.

Coverage can range from \$5,000 to \$25,000. Insurance generally includes restoration services, which come in two forms: 1) without limited power of attorney, where the consumer is provided with the necessary templates and forms and guided through the resolution process 2) with limited power of attorney, where the solution provider handles everything on behalf of the victim. The most common carriers in this space include AIG and Travelers, but several companies also provide in-house resolution services that are not backed by insurance carriers to cover restoration costs.

Conclusion

With consumers revealing tarnished confidence and negatively impacted relationships with breached organizations, institutions have more to worry about than patching security holes with IT investments and upgrades.

Data loss incidents severely hamper consumer trust, resulting in serious implications for customer loyalty and reputation. More than half of breach victims express diminished trust with the institution's ability to protect their information, while 30% state they would never purchase products again from that organization. With the exposure of highly sensitive information such as social security numbers, breached institutions are expected to go beyond basic notification protocols and demonstrate proof of steps being taken to ameliorate the situation.

The most relevant and appropriate action is for the breached institution to offer an identity fraud protection solution, which will address the security concerns of breach victims and minimize the risk of fraud. Breach victims express a strong preference for preventative fraud protection, compared to detection or resolution oriented solutions. Consumer data shows that 56% of breach victims favor a product that prevents the fraudulent use of their information. Due to the particularly difficult nature of new accounts fraud, prevention is especially important in mitigating any potential impact to the consumer.

Recommendations

Javelin recommends the following measures, which address consumer security concerns and expectations, to institutions in the event of a data breach:

- Thoroughly examine the types of data that have been exposed and assess the risk and action needed. If social security numbers or other highly sensitive information are compromised in the breach, it is strongly advised to offer a complimentary preventative fraud protection service for at least one year to affected customers and or/employees. Victims will expect the institution to take action on their behalf and minimize the potential risk of fraud.
- Given the wide variety of fraud protection solutions and varying features out in the market, companies should engage in comprehensive research of the different services available to understand whether they play a role in prevention, detection or resolution.
- Select a solution that is convenient and easy for the breach victim, in terms of enrollment and use, and provides greater emphasis on effectively *preventing* new accounts fraud.
- Understand that offering a breach solution is a best practice from a customer service standpoint. In other words, do not create a situation in which your customers and/or employees have to request fraud protection assistance. Take a proactive approach by offering the assistance up front.