White Paper

The Effect of Identity Fraud to Financial Services Organizations: Costs, Losses, Resource Requirements and Best Practices

Research provided by:

Richard A. Riley, Jr. and Timothy Pearson
Institute for Fraud Prevention
West Virginia University

and

Michael C. Smith
LexisNexis® Risk Solutions

LexisNexis®

The Effect of Identity Fraud to Financial Services Organizations: Costs, Losses, Resource Requirements and Best Practices

Abstract

Financial Institutions (FIs), like their customers, are victims of identity fraud. FIs suffer losses, expend costs and invest in controls to deter, prevent, detect and mitigate the likelihood and impact of identity fraud on their customers and themselves. This white paper can be seen as a resource for FIs to understand those losses, costs, resources being expended and current best practices associated with addressing identity fraud.

Understanding the Problem: Definitions and Overall Impact

Definitionally, identity theft occurs when an imposter or thief gains unauthorized access to credible personal identifying information of another person or group of people. Identity fraud occurs only when the information derived from identity theft is **used** for illicit purposes. Furthermore, identity fraud must involve perpetrators exploiting approved or accessed credit lines (derived from identity theft) for Financial Institutions (FIs) to sustain identity fraud write-off losses. Notwithstanding their legal and ethical responsibility to protect identifying information, the use of a victim's identifying information which result in illicit losses against the Financial Institution (FI) is a main concern to FIs. Some of the illicit losses are derived from:

- Credit and loans
- New checking accounts
- New credit cards, debit cards and retail card accounts
- Mortgages

Other illicit misuses of data include obtaining fraudulent:

- Identifying documents such as drivers licenses, passports, birth certificates, etc. (more of a means to commit identity fraud by alerting or stealing)
- Leases and rental contracts
- Contracts
- Employment
- Avoidance of arrest and criminal records

Generally, FIs are most concerned about losses associated with credit cards, loans, checking accounts, debit cards, mortgages and other financial transactions that are initiated and facilitated with fraudulent identifying information such as fake driver's licenses, passports, birth certificates and other identifying information. It is not the creation of these accounts that causes losses but the subsequent default on obligations created. Credit cards are used to make purchases and leave the FI with no ability to collect payment on the credit card. Checks are written on checking accounts to make purchases where no money exists in the account, and the FI is left with little to no hope of collection. Loans are secured on consumer goods but are subsequently defaulted on, leaving the FI will little recourse. The creditworthiness of the borrower is of critical importance to FIs but just as important are the honest representations of individuals seeking use of and credit from the FI and the systems in place at the FI to establish the irrefutable identity of the borrower or client.

However, FIs are not the only victim. Identity theft that evolves into identity fraud can impact FI customers as well as victimize those persons who have no prior relationship with the FI. What steps FIs take to prevent identity fraud against innocent consumers and what they do as an organization entrusted with societies' resources are critical to building and maintaining the trust of consumers and government regulators. In tough economic times, identity frauds that might have remained concealed for some time are more quickly discovered; identity-based frauds which are masked by high real estate prices, easy credit and rising stock markets are discovered more quickly.

Identity fraud criminals have their own concerns, including ROI calculations. Essentially the thief will attempt to invest time and resources in the expectation of a "return," illicit though it may be. Part of their return is dependent on the time period from inception of the fraudulent act until detection or the probability of detection is high enough that the criminal quietly disappears. To minimize the chances of detection, the predator might spread their transactions to improve their returns. This can be accomplished by executing transactions over a number of accounts or over an elongated period of time. Another alternative is to concentrate on larger accounts where missing dollars are less likely to be detected in a timely manner.

The Internet has created new opportunities for the identity theft/identity fraud criminal. Consider a well-spoken, business-savvy, discreet Russian and bright young tech star named "A-Z", a crack programmer and successful entrepreneur (adapted from Diaz, Allision, "Meet A-Z: The Computer Hacker Behind a Cybercrime Wave," USA TODAY, August 5, 2008; see also, Rezaee, Z and Riley, "Financial Statement Fraud," forthcoming from Wiley). A-Z is also a cyber-criminal and his customer base is mostly bad actors. A-Z's computer program called ZeuS helps cyber-gangs steal people's identity data and pull off web scams on a vast scale. In fall 2007, ZeuS was used to hijack $6 million. Here's the "short-story" version of how A-Z and his compatriots stole $6 million:

1. In summer 2007, a German gang skilled at pilfering online bank accounts forged a "partnership" with Russian hacker A-Z who created ZeuS, a versatile software tool for infecting PCs that is housed on a network server in Turkey.

   The partnership sent out waves of email spam carrying purported links to greeting cards, news stories and celebrity videos. Clicking on the hoaxed link installed generic ZeuS on your PC. Generic ZeuS has two tasks: (a) collect data typed on banking and other web pages; and (b) turn the PC into a "bot" that can be operated by other PCs remotely without the knowledge of the user.

2. The summer and fall are spent "harvesting" personal data from PC users with commercial accounts at banks that allow online cash transfers.

3. Targeted "fake" email is sent to bank patrons asking them to "click here" to reset their security codes. Those that fall for the ruse—thousands—have a custom version of ZeuS installed on their PCs.

4. Custom ZeuS tracks the PC user's keystroke activity and alerts the cyber-gang each time the PC user logs into their bank account. While the user is logged into their bank, one of the cyber-gangs "bots" completes a cash transfer ranging from $5,000 to $10,000 in a few seconds without the user's knowledge.

Within two weeks, the cyber-gang extracted $6 million from thousands of accounts at 20 of the largest banks in the USA, U.K., Italy and Spain. Authorities finally discovered the computer server holding key instructions for transferring funds in Turkey and shut the server down. The story of A-Z is part of a broader phenomenon referred to as "NetWar," a concept first outlined by John Arquilla and David Ronfeldt of the RAND National Defense Research Institute. This is the essence of NetWar: Cyber-criminals from Russia, Germany and Turkey, loosely combine for a short period to victimize banks and persons in the United States, England, Italy and Spain.

In a different cyber-case, researchers from U.K.-based security firm Prevx found a similar trove, a website used as a stash house for data from 160,000 infected computers; it was subsequently shut down. Contemporary cybercrime is like any other business. It behaves according to traditional business principles such as profitability, ease of use, risk management and emerging markets. Well defined relationships—even though temporary in nature—and business models are in place. A new class of cybercriminals freely and openly buys and sells malicious code and stolen data. These cybercriminals range from petty fraudsters who steal small sums in large quantities to individuals who attempt to steal large sums of money at one time (see "The Cybercrime Arms Race", September 17, 2008, Eugene Kaspersky, Head of Kaspersky Lab Virus Research).

It is in the best interest of identity thieves and fraudsters to go after targets such as FIs with high liquidity and the opportunity to extract assets from a distance and hopefully anonymously. Alternatively the identity thieves can steal the information and sell or exchange it with another party to make a profit without ever completing a fraud act (without taking part in existing or new account fraud). By distancing themselves, delegating tasks across various bad actors and layering transactions from the identity theft to the fraud act, fraudsters operate in jurisdictions where such behavior is often ignored and hope to avoid detection and escape by protecting their own identities.

FIs have always been a compelling target for thieves and swindlers simply because they are in a known location with very liquid, untraceable and highly portable cash assets, often in an electronic form. In recent years, the ease of online access and funds transfers has made FIs an even more attractive target. Gaining access to existing checking accounts is reported by some researchers to be the fastest growing form of identity theft. In contrast, new account frauds have waned a bit due to tougher screening at the application stage. However, a recent 2009 white paper by LexisNexis® and Javelin indicates the trend is back up again.[1]

In recent years, the ease of online access and funds transfers has made Financial Institutions an even more attractive target. Gaining access to existing checking accounts is reported by some researchers to be the fastest growing form of identity theft. In contrast, new account frauds have waned a bit due to tougher screening at the application stage. However, a recent 2009 white paper by LexisNexis® and Javelin indicates the trend is back up again.[1]

Synthetic identity fraud is becoming a more common type of identity fraud. Whereas "true-name" identity fraud corresponds to actual consumers, in a typical synthetic identity fraud, an identity fraudster uses a real or manufactured Social Security Number (SSN) and combines it with a fake name, a name not associated with the SSN. In most cases, the synthetic fraud doesn't hit the consumer's credit report. Alternatively, it could create a seemingly real identity which really should not and does not really exist—and that identity is relied upon by the bank. Chris Jay Hoofnagle, senior staff attorney to the Samuelson Law, Technology and Public Policy Clinic and senior fellow with the Berkeley Center for Law and Technology at the University of California argues that synthetic identity fraud has greater potential for serious financial damage to FIs since the synthetic identity does not impact a "real" person; thus, the risks and fraud losses rest solely with the FI. Institutions relying solely on credit reports would find synthetic name frauds in credit default buckets since discovery of the fraud requires more advanced detection processes.

Costs, Losses and Resource Requirements

The costs, losses and resource requirements estimates associated with identity theft and identity fraud are descriptive in nature, provide somewhat conflicting information based on the research methodology and data collection techniques and are somewhat anecdotal. In this section, we attempt to organize that information, knowing that the costs, losses and resource requirements, as of this point in time, are an area where additional work is required, and FIs could benefit from more comprehensive and standardized data repositories and reporting structures.

Losses Associated with Identity Theft

FIs are informed of data breaches regularly (oftentimes more than 2 times a week depending on customer volumes) through VISA/MC/Discover/AMEX (Card Associations). These data breaches do not always involve personal identifying information so the jury is still out concerning whether this is identity theft—it is often the theft of a person's credit card number, expiration date, security code and potentially name. If fraud were to happen on credit card accounts, for example, then the bank would likely write them off not as identity theft, but counterfeit or stolen card fraud. However, FIs decide based on their own risk assessment if they will monitor stolen accounts, block those accounts, notify customers and/or reissue cards or financial devices. The actual amount of lost confidential or personal information is staggering. Organizations are increasingly monitoring the fraud rates of breached customers and then using those rates (fraud incidents and dollars lost) to decide whether to notify customers while monitoring customers' account and transactional behaviors in the meantime.

Regulations in more than 35 U.S. states require that individuals (customers, employees, citizens, students, alumni, etc.) be notified if their confidential or personal data has been lost, stolen or compromised. Generally, these regulations require that when a breach occurs, organizations must notify all affected individuals, attempt to minimize downstream brand consequences, and put solutions in place to prevent a recurrence. Although the specific conditions for notification vary by state, organizations may not be required to notify individuals when the breached data is protected by encryption or the breach was stopped before information was wrongfully acquired.

The costs associated with identity fraud are directly tied to compromised personal information. Since January 2005, the Privacy Rights Clearinghouse has identified more than 250 million records of U.S. residents that have been exposed due to security breaches. According to the 2009 Annual Study: "U.S. Cost of a Data Breach" conducted by the Ponemon Institute, LLC, the total average cost of a data breach grew to $202 per record compromised in FY 2008, an increase of 2.5% since 2007 ($197 per record) and 11% compared to 2006 ($182 per record). Breaches are costly events for an organization; the average total cost per reporting company was more than $6.6 million per breach (up from $6.3 million in 2007 and $4.7 million in 2006) and ranged from $613,000 to almost $32 million.

- The cost of lost business continued to be the most costly effect of a breach averaging $4.59 million or $139 per record compromised. Lost business accounts for nearly 70% of data breach costs, up from 65% in 2007, compared to 54% in the 2006 study.

- Breaches by third-party organizations such as outsourcers, contractors, consultants and business partners were reported by 44% of respondents, up from 40% in 2007, up from 29% in 2006 and 21% in 2005. Per-victim cost for third party errors is $52 higher (e.g., $231 vs. $179) than if the breach is internally caused.

- Data breaches experienced by "first timers" are more expensive than those experienced by organizations that have had previous data breaches. Per-victim cost for a first time data breach is $243 vs. $192 for experienced companies. More than 84% of all cases in the 2007 study involved organizations that had more than one major data breach.

- Forty-nine percent of organizations exposed through a breach have reacted by creating additional manual procedures and controls. Of the technology options, 44% of companies have expanded their use of encryption technologies, followed by identity and access management solutions to prevent future data breaches.

- FIs suffer the highest rates of customer loss of 5.5%. This high rate reflects the fact that these industries manage and collect consumers' most sensitive data. Consumers may have a higher expectation for the protection and privacy of their personal records at FIs.

- Over 88% of all cases reported in 2008 involved incidents resulting from insider negligence.

- Legal defense and public relations costs increased.

- Lost and stolen laptops and mobile devices are a frequent cause of data breaches.
- FI firms were impacted most: The cost of a data breach for financial services organizations was 21% higher than average, demonstrating that organizations with high expectations of trust and privacy have more to lose from a data breach.

Losses Associated with Identity Fraud

The FTC complaint report for 2008 shows 1.22 million complaints related to fraud, identity theft and other consumer complaints—16% higher than the 1.05 million complaints in 2007 (www.ftc.gov/opa/2009/02/2008cmpts.shtm). Those consumers reported fraud related losses of more than $1.8 billion. There is some disagreement amongst researchers about the scope of the problem due to the nature of the survey technique and data collection process. In their work, Javelin indicated about 10 million identity frauds in 2008. This is from a self-reported survey where Javelin attempts to narrow their focus on the causes and effects of reported frauds.

According to FTC 2008 data, 52% of complaints were fraud complaints, 26% were identity theft complaints and 22% were classified as other types of complaints. Identity fraud losses to businesses and FIs totaled $47.6 billion and consumer victims reported $5 billion in out-of-pocket expenses. These costs include fraud loss write-offs, direct incremental costs, lost productivity, reduced customer confidence, customer attrition, negative publicity, fines, lawsuits, investigation and victim remediation.

Public media sources and researchers report the following statistics on identity fraud since 2001:

- "Banks Lost At Least $1 billion To Identity Thieves In 2002," MSNBC. www.msnbc.msn.com/id/3078480/
- According to the FTC in 2007, (www.ftc.gov/opa/2008/02/fraud.shtm), identity theft complaints have accounted for more than one-third of all fraud complaints they received from 2004-2006. Identity theft has been the number one fraud complaint filed with the FTC for the better part of a decade. The agency's yearly publication of its fraud complaints regularly finds identity theft outstripping all other categories. In 2007, the FTC reported that of 813,899 total complaints received in 2007, 258,427, or 32%, were related to identity theft. www.consumeraffairs.com/news04/2008/02/id_theft.html
- According to the FTC, total consumer fraud losses totaled $1.2 billion, with the average monetary loss for an individual at $349.
- The FTC's last official survey, released in November 2007, claimed 8.3 million Americans had been victims of identity theft in 2005. The agency recently announced that it would commission a new study of the experiences of identity theft victims, including their knowledge of remedies available to them under the law. www.ftc.gov/opa/2007/11/idtheft.shtm

- The 2003 FTC report estimated identity theft losses to Financial Institutions at $47 billion. www.ftc.gov/opa/2003/09/idtheft.shtm

"The FTC released statistics from its 2008 Consumer Sentinel Network Data Book showing that 313,982 people had their identities stolen last year, up from 162,000 reported in 2002. Twenty percent of the thefts were used to perpetrate credit card fraud, while 13% were used for phone or utilities fraud. Other categories included bank fraud, employment-related fraud, government documents or benefits fraud, and loan fraud. About 24% of thefts were used to perpetrate multiple types of fraud." "Consumer Sentinel Network Data Book," January-December 2008, issued February 2009

According to a recent survey from Gartner ("Financial Fraud Hit 7.5% Of Americans In 2008," Gartner, March 2009), around 7.5% of U.S. adults lost money to financial fraud last year, with a string of high profile data breaches the main cause. The survey of nearly 5,000 U.S. adults shows 14% had their credit card data misused, seven percent their debit card exploited, six percent said a new account had been opened in their name, five percent were the victims of money transfer fraud and four percent had checks forged. A data breach was cited as the reason for the fraud by 19% of victims, with 16% blaming the theft of their wallet and 13% online scams, such as phishing. Reported data breaches in the U.S. during 2008 were up 47% on the previous year, to 656, of which 78 affected FIs, according to a recent study from the Identity Theft Resource Center (ITRC). The Gartner survey shows that just a third of victims report crimes to law enforcement and about five percent contact the Federal Trade Commission. The reluctance to report identity theft related fraud may be contributing to poor conviction rates of less than 0.5%. Recently Rita M. Glavin, Acting Assistant Attorney General, Criminal Division, Department of Justice, testified at the House Homeland Security Committee hearing on PCI standards. As part of her testimony Assistant Attorney General Glavin reported that there are more than 2,000 active cases related to identity theft pending in the U.S. Attorney's Offices. She said there has been a 138.2% increase in identity theft convictions between 2004 and 2008.

According to a recent survey from Gartner, around 7.5% of U.S. adults lost money to financial fraud in 2008, with a string of high profile data breaches the main cause.

The Gartner report says financial losses are highest in the case of new account, credit card and brokerage fraud, with the average cost per incident totaling $1,097, $929 and $900, respectively. Victims of brokerage, credit card and debit card account fraud find it easiest to recover their losses, receiving an average of 100%, 86% and 77% of the funds stolen, respectively. In contrast, victims of new account fraud only recover 42% on average, for check forgery the figure is 48% and for checking or savings account fund transfer fraud, 54%. New account fraud is also the most difficult from which to recover, with 35% of victims suffering further from a damaged credit rating, which can take years to restore. Gartner says that fraud victims are twice as likely to change their online banking behavior and suggests PayPal has received a "big boost" as customers concerned by security are flocking to the service.

In 2005, ID Analytics reported that synthetic identity fraud accounted for 74% of the total dollars lost by U.S. businesses to identity fraud and 88% of all identity fraud "events"—for example, new account openings and address changes. 11.7% of successfully opened fraudulent account applications were opened using a real person's identity. The remaining 88.3% of the successfully opened fraudulent account applications appeared to be opened using a synthetic identity. Synthetic identity fraud also represented the majority of dollar losses: 73.8% of dollar losses were due to synthetic identity fraud, compared to 26.2% for true-name identity theft.

Javelin recently reported that ID theft is most likely caused by friends or relatives stealing paper-based documents. "The truth is, most known cases of fraud occur through traditional methods, when a criminal has direct, physical access to the victim's information." Javelin further reported that only 11% of the victims in 2008 were exposed through data breaches. In a challenge to the Javelin findings, on February 16, 2009, Rob Douglas (www.identitytheftblog.info/identity-theft/javelins-identity-theft-report-misleading/1233) indicated that 65% of victims were unable to locate the source of their breached information. It is likely that they were victims whose information was lost in a skimming attack or a reported (or unreported) data breach. The various reports and evidence supporting claims of costs and trends in identity fraud need to be reexamined and synthesized to get a handle on the scope of the problem.

Reputational costs

According to the Ponemon Institute, LLC (2007):[2]

- Trust may be intangible and hard to quantify, but the result of breaking that trust is clear as the cost of lost business grew more than 30% since 2006.
- Organizations that have built their brand on trust have more to lose from a data breach demonstrated by the 21% higher costs for FIs compared to an average breach.

Best Practices in Deterrence, Prevention, Detection and Mitigation

Since 2001, FIs have been tasked to prevent identity fraud associated with terrorist financing, money laundering and to mitigate the impact of identity fraud on individuals. Filing of Suspicious Activity Report (SARs) is critical to filter unusual or suspect transactions. On December 4, 2003, President Bush signed into law the **Fair and Accurate Credit Transactions Act (FACTA)** to provide consumers with increased protection from identity theft. Six agencies were involved in drafting the rules: the Treasury Department's Office of Thrift Supervision, the Office of Comptroller of the Currency, the FDIC, the FTC, the National Credit Union Administration and the Federal Reserve System. The Red Flags Rule amended FACTA in 2008 and requires FIs to get more serious about protecting consumers from identity fraud. The rules contain three parts. First, covered entities must create a written identity theft program designed to detect, prevent and mitigate identity theft in connection with certain covered accounts (the "Red Flags Rule" or the "Rule"). Second, users of consumer reports must adopt policies for verifying identity when they receive a notice of address discrepancy from a consumer reporting agency. Third, debit and credit card issuers must implement procedures to assess the validity of address changes under certain circumstances. Red Flags Rule applies to FIs, including banks and credit unions as well as other business entities such as auto dealers, mortgage brokers, utility companies and telecommunications companies. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking and savings accounts, and in some cases business accounts where this is a foreseeable risk of identity fraud.

FIs must build transaction level, processes and organizational initiatives to avoid identity theft and related fraud losses. FIs are required to have Customer Identification Programs (CIP), Know Your Customer (KYC) programs and systems in place regarding terrorist financing and anti-money laundering. CIP requires, at a minimum, reasonable procedures for (i) verifying the identity of any person seeking to open an account; (ii) maintaining records of the information used to verify the person's identity; and (iii) determining whether the person appears on any lists of known or suspected terrorists provided to the Financial Institution by any government agency. However, while these systems are steps in the right direction, they cannot be relied on exclusively to protect against identity fraud.

The "Red Flags Rule" requires identity theft prevention programs to include "reasonable policies and procedures" to identify relevant red flags and incorporate them into the program, to detect those red flags, to respond appropriately when red flags are detected and to ensure that the program is updated periodically. ID theft/fraud red flags may include the following:

- An application that appears to have been forged, altered or destroyed and reassembled.
- A consumer report that includes a fraud alert, credit freeze or address discrepancy.
- A change-of-address notice that is followed shortly by a request for a new credit card, bank card or cell phone.

The Red Flags Rule amended FACTA in 2008 and requires Financial Institutions to get more serious about protecting consumers from identity fraud. The rules contain three parts:

(1) Covered entities must create a written identity theft program designed to detect, prevent and mitigate identity theft in connection with certain covered accounts (the "Red Flags Rule" or the "Rule").

(2) Users of consumer reports must adopt policies for verifying identity when they receive a notice of address discrepancy from a consumer reporting agency.

(3) Debit and credit card issuers must implement procedures to assess the validity of address changes under certain circumstances.

- A Social Security Number supplied by an applicant that is the same as that submitted by another person opening an account.
- An address or telephone number supplied by an applicant that is the same or similar to the account number or telephone number submitted by an unusually large number of other persons.
- Notification of the Financial Institution or creditor that the customer is not receiving account statements.
- Use of an account that has been inactive for a reasonably lengthy period of time.

Simply adopting the Red Flags Rule is the minimum compliance baseline. Proper mitigation methods extend beyond the basics of the Red Flags Rule. (Gartner Report "Best Practices in New Account Fraud Detection." Gartner Report ID: G00155118. February 12, 2008, Avivah Litan.) FIs exposure to identity theft and subsequent fraud also comes from online access to databases and transaction processing. More than 10 million Internet users worldwide were hit with identity fraud-related malware last year, according to a new estimate from Panda Security, one of the world's leading creators and developers of technologies, products and services for keeping clients' IT resources free from viruses and other computer threats at the lowest possible Total Cost of Ownership. The number of computers infected with active programs designed to steal personally identifiable or financial information that can be used for identity fraud, such as banker Trojans for stealing bank account information, rose by 800% from the first half of the year to the second half. The number of users who have been actively exposed to identity fraud malware is about 1.1% of the worldwide population of Internet users (news.cnet.com/8301-1009_3-10193025-83.html). What are financial institutions doing to stop unauthorized access? They are implementing best practices in information handling:

- Enhancing authentication and verification policies and procedures.
- Enhancing protection of all PII (Personal Identifying Information).
- Limiting access to PII by employees on a need to know basis.
- Properly disposing of sensitive documents and electronic data.

FIs are helping customers with PII exposure by:

- Providing documents and information so that the victim can file a fraud affidavit.
- Providing the victim with transaction details and credit application information, so that the victim can proceed with mitigation.
- Providing a letter of clearance and stopping all collection action against the victim when fraud is determined.
- Supporting law enforcement efforts to investigate the identity theft case.
- Preparing a comprehensive, intelligent and timely breach notification for the affected parties.

- Offering credit or even identity monitoring services to affected customers, or taking these mitigation steps behind the scenes on the customers' behalf.

The pressure today is on authentication. Besides guidance from the FFIEC, regulations like Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) focus on protecting personal information. Translation: Authentication methods need to be strengthened, or FIs may not be able to reasonably argue that they have taken the necessary steps to protect personal information, especially when that information is subsequently used to perpetrate identity fraud.

Financial Institutions are particularly vulnerable to privacy violations. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. FIs should implement multifactor authentication, layered security and other controls reasonably calculated to mitigate those risks. FIs offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. FFIEC guidelines focus on the online environment, so one main concern is that instances like authenticating a caller who calls a FI to request that a new user with account privileges be added to an account may not be prevented. For example: a criminal who gains access to an account and then adds him/herself to the account and subsequently requests an address change be made or a new financial access device sent to another address whereby the criminal has access is extremely common and this is a situation where more rigorous fraud authentication methods can attempt to solve. Increasingly, more advanced schemes are being perpetrated whereby a bank may consider Automatic Number Identification (ANI) and a SSN to be meeting FFIEC authentication requirements for callers to telephone call centers. However ANI spoofing (or using someone else's phone line and tricking the ANI system) to make a call seem to come from a customer instead of a criminal is becoming more problematic. Authentication in an Internet Banking Environment Federal Financial Institutions Examination Council, http://www.ffiec.gov/pdf/authentication_guidance.pdf.

Authentication methods need to be strengthened, or Financial Institutions may not be able to reasonably argue that they have taken the necessary steps to protect personal information, especially when that information is subsequently used to perpetrate identity fraud.

Even the USA PATRIOT Act focuses on authentication. The USA PATRIOT Act focuses on verification at account origination, whereby FFEIC focuses on authentication of existing relationships—Section 326 of the Act requires FIs to verify a user's identity during account origination. This oftentimes involves the FI comparing key application fields like first name, last name, address, city, state and SSN to electronic databases that hold reliable intelligence on the applicant. Increasingly FIs and financial services organizations are utilizing pattern recognition to determine the likelihood of the applicant (or application) resulting in identity fraud or misrepresentation (from which losses they would write-off 6-12 months from date of account origin). These systems use analytics to identify fraud patterns from historical data, translate fraud patterns into rules or scoring algorithms, and are deployed to identify new instances of fraud in real-time. Advantages to these technologies range from reduced operating costs derived from on-boarding new accounts to reductions in application fraud (which translates to stronger compliance). Using this technology makes sense because it solves multiple problems: identity fraud, customer convenient, operational costs and compliance.

The average consumer will probably encounter something like knowledge-based authentication, which still attempts to balance an acceptable level of convenience and risk tolerance. As consumers move through new account originations and within their existing account online sessions, they will be asked for more personalized information as they initiate new activities. Using shared information is a solution that is easy to administer, yet hard for criminals to beat; however even this method is not free from breach and customer forgetfulness.

In addition to the above methods, organizations are addressing online application fraud channels by monitoring IP address usage associated with a customer and registering new applicants, after successful identity credentialing, with machine based biometrics, like computer device identification. Internal negative files, or hotlists, are being deployed as a best practice by FIs, however, even these systems need updating because previous bad addresses or phone numbers are recycled over time.

Organizations need the appropriate and reliable identity related data and technology to verify and authenticate consumers and customers, a streamlined process to do this effectively without unnecessary costs and customer delays, and need to consider the compliance regulations that they are held to.

The broad umbrella of identity theft and fraud prevention fits Federal Financial Institutions Examination Council (FFIEC) guidelines on multi-factor authentication to bring in the element of authenticating a customer who completes risky transactions. Federal regulators recognize that banks need some guidelines for fighting identity theft:[3]

- Banks should take “appropriate” steps to ensure the accuracy and truthfulness of information on application forms. For example, a bank could check to see if a ZIP code and area code match.
- Banks “should verify customer information before executing an address change” and send confirmation of an address change to the old address and new address.
- If a customer orders a new credit card or box of checks and at the same time makes an address change, the bank “should verify the request with the customer.”
- Banks shouldn’t give out sensitive customer information over the phone unless the caller knows a password or can answer a question that an impostor shouldn’t be able to answer.
- Some victims of identity theft put a “fraud alert” on their credit records, asking that someone make a confirming phone call whenever someone tries to open an account in that person’s name. The Fed’s letter asks banks to make that phone call.

Historically, guidance provided by regulators does not consider the fraud risk management approach that banks have to balance with every new account opened or existing account request. In addition, with the exception of the Red Flags Rule, there is not a lot of specific guidance given to banks (the previous page bullets are very generic) so they have to utilize their best fraud approaches, considering they do not have infinite budgets and customers do not want to be inconvenienced.

According to Gartner (March 2009), organizations must employ defense-in-depth, using multiple layers of security controls as part of an integrated security program to prevent, detect and respond to attacks that would evade common standalone security technologies. Best practices for defense-in-depth include:

- Using Network Intrusion Prevention Systems (NIPS) at all network perimeters and between key network segments to block known exploit attempts and some forms of anomalous activity.

- Monitoring and analyzing of ingress (inbound) and egress (outbound) firewall traffic logs in real-time to detect abnormal activity that could signify a compromised host.

- Monitoring and analysis of host and application logs in real-time on critical systems and network devices to detect exploit attempts, password grinding and anomalous behavior by users and applications.

- Using host-based security software including Host IPS (HIPS), anti-virus and anti-spyware to provide added protection beyond native host capabilities.

- Using Security Information Management (SIM) to correlate numerous security events from across networks and to detect more sophisticated attacks.

- Conducting regular vulnerability scans, assessments and remediation (such as patching, removing unnecessary services, etc.) to minimize exposure to exploits.

- Performing penetration tests to validate defenses against the latest hacking methods.

From an investment and cost-benefit perspective it can be difficult for FIs to justify significant resources dedicated to combat identity fraud. Possibly the greatest cost from a data breach leading to identity theft is customer turnover; the cost to brand and corporate reputation can be the most long lasting effect. Banks must take a risk-based approach, realizing that they cannot stop all the identity fraud, but if they can stop the majority, their systems are sufficient. Operational costs come into play as well. For example, a bank may be able to stop 95% of fraud if they just review applications with a fine toothed comb, but customers (and the bank) want to facilitate instant decisions from both applying for an account to completing a "risky" transaction (using credit cards, cashing checks, changing an address, performing a balance transfer, adding a spouse to an account, etc.). These types of account behaviors are consistent with those of identity fraud perpetrators, however, ordinary customers want instant results, even though they understand and consider that the reason for the delay or additional step is for their security. It's a bit odd how customers are impatient this way. However, it is suggested that nine out of ten consumers report they are prepared to sacrifice convenience in favor of stronger security to protect online bank accounts.

Conclusion

As stated in the beginning of this paper, it is clear that Financial Institutions, like their customers, are victims of identity fraud. FIs suffer losses, expend costs and invest in controls to deter, prevent, detect and mitigate the likelihood and impact of identity fraud on their customers and themselves. In this document, we have carefully discussed the losses, costs and resources being expended and current best practices associated with addressing identity fraud as well as the existing research and regulatory requirements. It is clear that FIs must find ways to create synergistic relationships in its use of identity related data to protect its customers and themselves from identity theft and fraud. By incorporating best practices and available data analytic tools, FIs can provide enhanced protection from fraud losses and costs.

End Notes

[1] "Stopping Fraud Where It Starts: The Value of Analytics in the Onboarding Process," research provided by Javelin Strategy & Research; July 2009; solutions.lexisnexis.com/forms/FS09ChngFraudJavFraudWhtPap704?source=LK_risk-fraudpoint.

[2] Source: "2007 Annual Study: U.S. Cost of a Data Breach Understanding Financial Impact, Customer Turnover and Preventative Solutions," Benchmark research conducted by Ponemon Institute, LLC, © 2007 PGP Corporation and Vontu, Inc.

[3] "Fed to Banks: Take Basic Steps to Stop Identity Theft," authored by Holden Lewis, Bankrate.com, Posted: May 15, 2001: SUBJECT: Identity Theft and Pretext Calling, FEDERAL RESERVE DIVISION OF BANKING SUPERVISION AND REGULATION SR 01-11 (SUP), April 26, 2001, http://www.federalreserve.gov/boarddocs/SRLetters/2001/sr0111.htm

For more information, visit risk.lexisnexis.com/fraud or call 866.858.7246.

For more information, visit risk.lexisnexis.com/fraud or call 866.858.7246

About LexisNexis

LexisNexis® is a leading global provider of content-enabled workflow solutions designed specifically for professionals in the legal, risk management, corporate, government, law enforcement, accounting and academic markets. LexisNexis originally pioneered online information with its Lexis® and Nexis® services. A member of Reed Elsevier, LexisNexis serves customers in more than 100 countries with more than 18,000 employees worldwide.

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions is the leader in providing essential information that helps advance industry and society. Building on the legacy of proven LexisNexis® services from the past 30 years, our cutting-edge technology, unique data and advanced scoring analytics provide total solutions that address evolving client needs in the risk sector while upholding high standards of security and privacy. LexisNexis Risk Solutions serves commercial organizations and government agencies and is comprised of several affiliated corporations, each offering premier customer-focused solutions. For more information, visit risk.lexisnexis.com.

LexisNexis®