Information Security News & Education

March 2010

10 FACES OF FRAUD

Old and New Schemes Target Banking Institutions and Their Customers

Also Inside

- Top 9 Breaches of 2009
- ATM Fraud: 7 Growing Threats to Financial Institutions
- Top 8 Security Threats of 2010

Interview Excerpts

- ID Theft Threats to Watch
- Gartner's John Pescatore

Interactive Features

- Data Breach Timeline
- Failed Banks Map

BANKINFO SECURITY®

BANK INFO SECURITY®

Facing Fraud in All its Forms

Tom Field

Welcome to our special RSA Conference edition of “10 Faces of Fraud,” our compilation of articles, insights and features from Information Security Media Group (ISMG), publisher of BankInfoSecurity.com.

It’s a dubious distinction, but 2009 was a banner year for fraud, and 2010 doesn’t look any different. The Heartland Payment Systems data breach stole the headlines, but there were scores of lesser-known crimes.

In this special compilation, we present some of our most popular fraud-related content, including:

- ATM Fraud: 7 Growing Threats to Financial Institutions;
- Top 8 Security Threats of 2010;
- 10 Faces of Fraud: Our cover story.

We’ve also included some interview excerpts with the likes of Gartner’s John Pescatore, as well as some entries from our ISMG blogs. And don’t miss the timeline of 2009’s top data breaches involving financial institutions.

Also, make sure you attend our own RSA Conference presentation, The State of Banking Information Security 2010, on Tues., March 2, starting at 2:30 p.m.

If this is your first exposure to either ISMG or the RSA Conference, then welcome. Please don’t hesitate to say hello to me or any of our team at or after the event.

Best,
Tom Field
Editorial Director
Information Security Media Group
tfield@ismgcorp.com

iSMG
INFORMATION SECURITY
MEDIA GROUP

10 Faces of Fraud

Editorial Staff

Tom Field, Editorial Director
Howard Anderson, Managing Editor
Eric Chabrow, Managing Editor
Linda McGlasson, Managing Editor
Upasana Gupta, Contributing Editor
Karyn Murphy, Contributing Editor

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries. This information is used by ISMG’s subscribers in a variety of ways — researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

4 Independence Way
Princeton, NJ 08540
Phone: (800) 944-0401
Email: info@ismgcorp.com

www.ismgcorp.com
www.bankinfosecurity.com
www.cuinfosecurity.com
www.govinfosecurity.com
www.healthcareinfosecurity.com

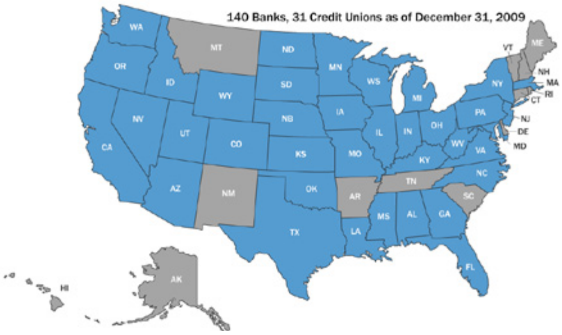
contents

Also in this Issue...

From Our Blogs

Interactive Features

Interviews



Top 9 Breaches of 2009

Here's the chronological list of the biggest breaches to affect financial services in 2009.

BY LINDA MCGLASSON

The top breaches of 2009 can be described in many ways, but the first word that comes to mind is "big."

With the announcement in January of the breach that surpassed the 2005 TJX breach, Heartland Payment Systems leads all of the hacks that hit or affected the financial services industry in 2009.

Here's the chronological list of the biggest breaches of 2009, and updates in the various cases since they were first announced:

1. Heartland Payment Systems

Princeton, NJ
Date: January 20, 2009
Records Taken: 130 million credit and debit card account numbers
Heartland Payment Systems announced on Jan. 20 that its network had been breached. The payment processor handles transactions for 250,000 merchants. Subsequently, it was revealed through indictments that 130 million credit/debit cards were compromised by the breach. While the outcome of several class action lawsuits has not been decided yet, the criminal accused of perpetrating the hack, Alberto Gonzalez, of Miami, FL, was indicted in August and is prepared to plead guilty. Financial institutions will watch closely the developments in the class action suits as they move through the courts in 2010.

> **"A network of thieves withdrew $9 million from 130 ATMs in 49 cities around the world just after midnight on November 8 with cloned cards created from stolen data taken in the RBS WorldPay hack."**

2. RBS WorldPay

Atlanta, GA
Date: November 2008/February 4, 2009
Records Taken: 1.5 million credit and debit cards

In February 2009 the FBI continued to search for suspects in what was being called a well-orchestrated ATM card scam, when the true extent of RBS WorldPay's hack was revealed. In a news report on February 4, FBI law enforcement said that a network of thieves withdrew $9 million from 130 ATMs in 49 cities around the world just after midnight on November 8 with cloned cards created from stolen data taken in the RBS WorldPay hack. Eight men from Eastern Europe were indicted for the crime in November 2009 and face stiff fines and lengthy jail sentences if convicted.

3. Countrywide Financial

Fort Worth, TX
Date: May 4, 2009
Records Taken: 4,000 account numbers

A man posing as an Air Force reservist seems to have gotten thousands of account numbers from Countrywide Financial in Forth Worth, TX. The investigators tracked the case to his accomplice, a customer service rep. The Air Force impostor stole $500,000.

4. Chase Bank

New York, NY
Date: May 18, 2009
Records Taken: Unknown

Four Romanian men were arrested in Florida after being accused of skimming a Central New York Chase Bank's ATMs. Police say several customers who used the ATM at a Chase Bank in Cicero later found cash had been withdrawn from their accounts from ATMs in New York City, totaling about $40,000. A skimmer was found in the card slot of the machine.

5. Network Solutions

Herndon, VA
Date: June 8, 2009
Records Taken: 573,000 credit and debit cardholders information

A data breach at Internet domain administrator and host Network Solutions compromised personal and financial data for more than 573,000 credit and debit cardholders. To add more pain to the breach, Network Solutions says it was PCI compliant at the time of the breach.

The breach was the result of hackers planting rogue code on the company's Web servers used to host mostly small online stores, intercepting financial transactions between the sites and their customers.

6. American Express

Phoenix, AZ
Date: July 7, 2009
Records Taken: Thousands of card numbers

Two Phoenix men are accused of stealing thousands of American Express card numbers and swindling more than $1 million dollars from customers. Police discovered during their investigation that a former employee had not only worked as a computer database analyst for American Express; he was one of the few who could have possibly downloaded all of their account holders information, including the PIN numbers used to access money from ATM machines at the different banks, according to court records.

“A computer technician was indicted in New York Supreme Court, charged with stealing the identities of more than 150 Bank of New York Mellon employees and using them to steal more than $1.1 million.”

7. Capitol One Bank

Minneapolis, MN
Date: September 6, 2009
Records taken: Unknown number of bank customer accounts

Prosecutors in Minneapolis say between July 2008 and April 2009 a crime ring purchased the personal information of Capitol One Bank customers from an online source in the Ukraine. It says the group then used the information to create counterfeit credit card accounts, withdrawing more than $652,205.49 from more than 170 ATMs throughout the Twin Cities. Eleven people have been charged in the counterfeit credit card scheme, eight of them are in custody.

8. PayChoice

Moorestown, NJ
Date: October 15, 2009
Records Taken: Unknown

PayChoice, a New Jersey-based payroll processor, alerted its online customers on October 15 that its network had been breached for a second time in less than a month. The payroll processing company warned its customers by email about the new breach after some clients reported “phantom” employees showing up on their payrolls.

9. Bank of New York Mellon

New York, NY
Date: October 28, 2009
Records Taken: 150 identities of employees

A computer technician was indicted in New York Supreme Court, charged with stealing the identities of more than 150 Bank of New York Mellon employees and using them to steal more than $1.1 million from charities, non-profit groups and other entities.

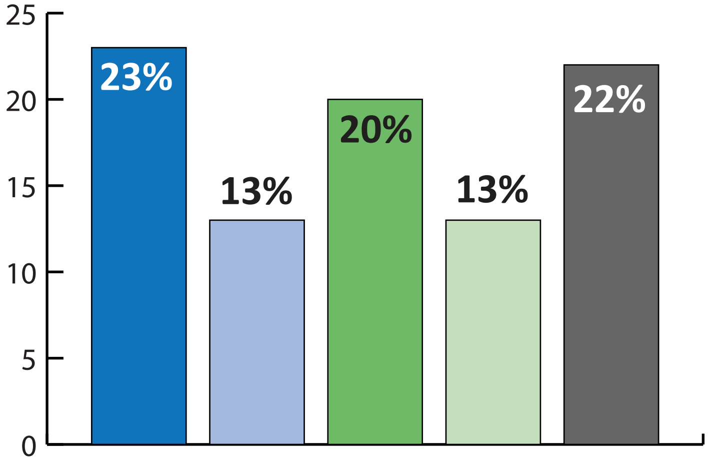
Adeniyi Adeyemi, a 27-year-old man from Brooklyn, was charged with grand larceny and identity theft. Prosecutors say Adeyemi worked in the bank’s Information Technology Department and committed the crimes between November 2001 and April 30, 2009. He is accused of stealing the identities of dozens of employees and using them to open more than 30 bank and brokerage accounts with several financial institutions including E*Trade, Fidelity, Citi, Wachovia and Washington Mutual. ■

Read the complete article online:
http://www.bankinfosecurity.com/articles.php?art_id=2001

> “Too many resources focused on regulatory compliance, not enough resources available for security and risk management related tasks”

The biggest challenge to mitigating security risks as indicated by respondents to the Banking Information Security Today™ 2009 Survey

23% - Insufficient budget
13% - Lack of competent resources
20% - Lack of tools and technologies
13% - Not enough buy-in from senior management
22% - Too many resources focused on regulatory compliance, not enough resources available for security and risk management related tasks



Find out how changes in the economy and widespread data breaches have affected responses this year

Presented at RSA Conference 2010:

Lessons Learned: The State of Banking Information Security 2010

Catalog ID: BUS-107
Date: Tuesday, March 02
Time: 2:30 PM
Room: Orange 302

Highlights from the annual Banking Information Security Today™ Survey, which takes the pulse of the financial community on topics such as:

* Rising threats
* Business priorities
* Emerging technologies
* Regulatory compliance

2009’s survey showed how banking institutions were fighting back against the recession. Results were widely embraced by the banking/security community, and have led to subsequent studies.

Can’t attend? Missed the session? Please visit BankInfoSecurity.com/RSA2010

Presented by Tom Field, Editorial Director of Information Security Media Group. An award-winning journalist with over 20 years experience in newspapers, magazines, books, events and electronic media, Field has developed and moderated scores of podcasts, webcasts, roundtables and conferences.

Selected as a distinguished speaker for RSA Conference 2010

BANK INFO SECURITY®

ID Theft Threats to Watch in 2010

Interview with Jay Foley of the Identity Theft Resource Center

Listen to this interview online >

BY TOM FIELD

Financial scams and incidents of medical identity theft are on the rise—and they're among the main threats to business and consumers in 2010.

This is the warning from Jay Foley, executive director of the Identity Theft Resource Center. In an exclusive interview, Foley discusses:

- The major ID theft threats and trends for 2010;
- The industries most at risk;
- What information security professionals can do to help prevent ID theft.

Responding to an explosive rise in identity theft crimes, Jay and Linda Foley established the Identity Theft Resource Center (ITRC) in 1999 in order to provide education and victim assistance to consumers and businesses. As executive director of the ITRC, Jay is today recognized nationally as an expert on identity theft issues.

Jay Foley

TOM FIELD: Now Jay, you have got new research out about the trends as we look into 2010. Just to give our audience a bit of a teaser, what do you see as the major trends of the New Year?

JAY FOLEY: Well, first and foremost we are going to see a lot more scams. Because of the tough economic times, we are seeing a lot of scammers come out of the woodwork and try to suck you into this quick job, that quick job, here make a little extra money, and invariably what happens is you find yourself on the hook for greater debt and greater problems because you went to work with these scammers.

Other things that we are seeing out there is that we are going to see an increase in medical identity theft. A lot more people are having trouble making ends meet, and one of the first things that seems to slip is going to be medical insurance. ' I haven't got medical insurance, so what I do is

I go down to the hospital and I give them somebody else's name and Social Security number, and I piggyback on their insurance.' It is becoming more and more of a thing, and it is becoming more and more alarming.

FIELD: Jay, what do you see as the challenges for information security professionals that are charged with helping these organizations do a better job protecting critical data?

FOLEY: First and foremost, they need to realize the biggest threat is not actually coming from outside the system. The numbers come out almost every year, and they have said for the past eight or nine years that 70% of all hacking happens internal to the company. It is somebody within your company that is going places who should not be in your data, not somebody outside the company.

A little more audit focus, a little more control focus as to who is going where and what they are doing needs to be addressed by each and every IT professional out there. You need to know who is going where and what they are doing and why they are doing it. You need to set up established parameters for who gets to go into the data.

FIELD: Now you have mentioned healthcare here a couple of times, Jay. As you look at the risks, are there any specific industries or even government agencies that you find to be at greater risk of identity theft than others?

FOLEY: If I were going to categorize the most sensitive industries, the first one I would go at would be the payment industry, the payment services industry, and that is the companies that process credit card and debit card transactions. Why? Because that is where the money is right at the moment. If a thief can get into your software and can get into your data, they have ready cash right there at their fingertips.

FIELD: Now you have mentioned healthcare here a couple of times, Jay. As you look at the risks, are there any specific industries or even government agencies that you find to be at greater risk of identity theft than others?

FOLEY: If I were going to categorize the most sensitive industries, the first one I would go at would be the payment industry, the payment services industry, and that is the companies that process credit card and debit card transactions. Why? Because that is where the money is right at the moment. If a thief can get into your software and can get into your data, they have ready cash right there at their fingertips.

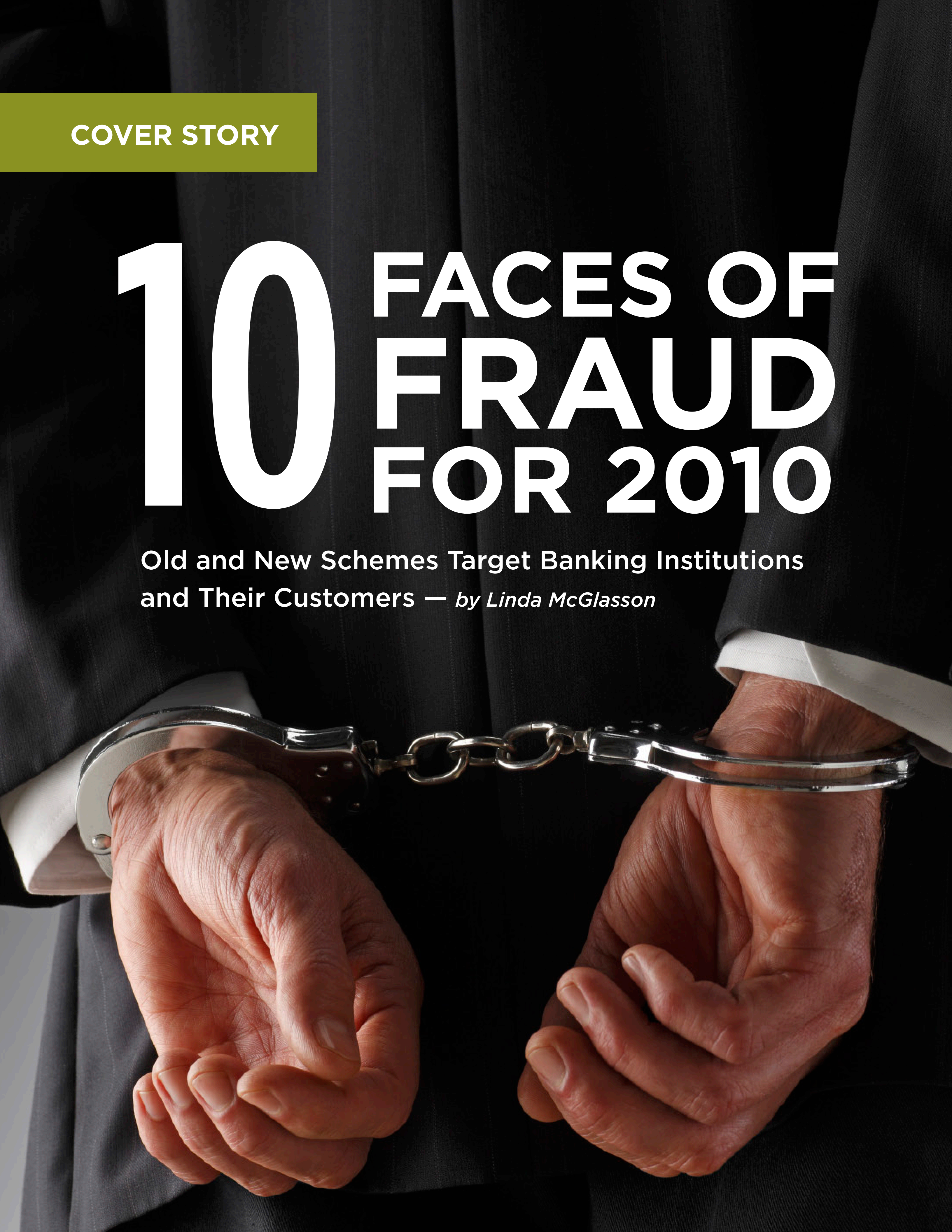
If we don't take the steps now to clearly delineate a security policy for this information, we are going to have two types of breaches. We are going to have those breaches like the Farrah Fawcett breach, where people actually broke into her medical records who had no business being there, and that information got blared out to the tabloids. Or we are going to have those that are going to get in there and are stealing the information out of your medical record and using it to create fraud, debt and general havoc in your life. ■

Read the complete interview transcript online:
http://www.bankinfosecurity.com/articles.php?art_id=2031

COVER STORY

10 FACES OF FRAUD FOR 2010

Old and New Schemes Target Banking Institutions and Their Customers — *by Linda McGlasson*



“The more things change, the more things stay the same.” This old saying holds true when it comes to the different types of fraud hitting financial institutions.

In 2009, institutions were hit from every angle with fraud schemes—some were old, and some were new variations. Here is a roundup of the 10 predominant types of fraud that institutions and their customers can expect to see in 2010, according to industry experts.

1. ACH and Wire Transfer Fraud

The attacks against small and medium businesses in the ACH channel in 2009 were a wake-up call to institutions for the New Year. Businesses and institutions alike suffer when fraudsters penetrate and pilfer accounts via hacking into electronic transactions.

“It started in earnest in 2009 and will only get worse in 2010 until banks put effective controls and fraud detection in place,” says Gartner analyst Avivah Litan. “It is hard to tune fraud detection systems to detect this fraud in a timely manner—especially wire fraud, since the data in a wire transfer instruction is not structured,” she says. But good fraud detection systems can catch most of this activity.

2. Attacks on Institution Networks

The level of protection provided transaction processing networks is often overlooked by institutions when it comes to servers outside of the “protected networks,” says Mike Urban, fraud director at Fair Isaac, the provider of FICO credit scoring.

“I’ve seen this particularly with vendor-managed servers where their security standards may not be at the level practiced by the institution where they are deployed, including password management and patch management,” Urban says. Identifying and managing all devices on corporate networks and protected transactional networks are critical to reducing the attack surface and eliminating weak links, he stresses.

3. ATM Skimming

There have been multiple stories this year in the U.S. about ATM skimming crimes. Experts say this particular form of fraud will continue to grow, as criminals are targeting U.S. financial institutions with technologies shared from Eastern Europe. “We should also expect that other ATM frauds such as card or cash trapping and lower quality skimming devices will continue to be a problem,” notes Fair Isaac’s Urban. Criminals will also keep pressure on older point of sale (POS) terminals that are not PCI compliant, he adds.

4. Credit Account ‘Bust-Outs’

The bad economy has given rise to many types of fraud in the past couple of years, but credit “bust-outs” have been around for some time. This fraud type made the list earlier this year, but Debra Geister, director, Fraud Prevention &

Compliance Solutions at Lexis-Nexis, says the trend is still very much active in any bank she's talking with now. "By definition, credit bust-out schemes are a combination of a credit and fraud problem, although many organizations are not always sure where the losses sit—or who might be the party responsible," Geister says.

5. Variations on Phishing Schemes

There have been many phishing attacks against financial institutions in 2009, so much that the Anti Phishing Working Group cites a 600 percent increase in overall phishing attacks over 2008. But there are more insidious types of attacks hitting institutions and their customers now, say experts.

Fair Isaac's Urban says businesses will be targeted with spear phishing and hacking efforts to compromise online banking credentials. Why they're targeting businesses, he says, is because "Criminals can then target those accounts and initiate money transfers via wires or ACH to steal large sums of money at once or over time." Business checks will also be targeted in counterfeit check scams, he adds.

"Fraudsters are using more realistic emails and other points of contact to try to entice credentials from victims," Eisen notes, including the SMS approach. SMS was considered to be a solution to unauthorized account access, Eisen says, "Since it was assumed sending a one-time use password to a cell phone would cause a challenge for fraudsters trying to gain access to accounts." Instead, it has begun to offer them a new way to scrape credentials. "This happens because customers don't expect to be targeted in this way and have accepted the practice as safe when they see a message that appears to be from their bank," Eisen says.

6. Check Fraud on Rise

It seems that everyone is using debit and check cards these days, and although paper check volumes are continuing to fall, Urban says the dollar losses to check fraud continue to rise. "Online banking account compromises contribute to check fraud when criminals can see cleared check images and identify sequence numbers," he says. One reason for the continued proliferation of this fraud is that there is easier access to check paper stock and cheaper printers and scanners to create fakes.

Eisen says one area institutions should look to lock down is the check image viewing online ability for customers. "It's a one-stop shop for data harvesting. Online checks offer visibility to an unauthorized view of the account number, personal information including the social security number (on checks in 19 states)."

7. Insider Crimes

This year has witnessed several widely publicized insider fraud crimes uncovered at institutions, and next year doesn't look any better. Tom Wills, Security and Fraud senior analyst at Javelin Research, sees the definition of "insider" has expanded as a wider variety of parties interact with institutions via their computer network. "RSA calls this the 'hyperextended enterprise,'" Wills notes. An insider can be thought of as anyone with authorized access to the bank's network resources, Wills stresses, "Not only employees and contractors of the institution, but those of suppliers and partners as well."

Internal fraud will continue at institutions and their partners, adds Fair Isaac's Urban, "where key information is compromised and used for personal use or sold to criminals who will perpetrate fraud on the institution or its customers.” Many of these schemes will fall apart in a similar manner to the investment schemes over the last year, when financially pressured consumers are more diligently monitoring their accounts or come in looking to withdraw the money from those accounts.

8. Mobile Phones

With nearly every bank and credit union throwing their hat into the mobile banking ring, the threat of mobile phone fraud is cause for concern. This crime is still in its infancy, but experts expect the risk will increase as malware applications are designed and spread onto mobile devices. Urban sees the most likely way fraudsters will target the mobile phones is through Trojans. “These Trojans will compromise information on the phones which may include online banking account information as well as other data stored on the phone. These compromises will be similar to the attacks on computers,” Urban says. The major difference will be the sheer number of mobile devices and operating systems in the market today, as compared to a dominant computer operating system, such as Microsoft Windows. Another reason to fear mobile phone fraud is that anti-virus and anti-malware applications are not as mature on mobile devices as they are on computers.

9. Online Applications

The ease of customer applications over the web comes with another set of headaches: Application fraud, which experts see as a growing area for criminals. Lexis-Nexis’ Geister says that alternative channel application crimes, including the Internet, Kiosk and point of sale channels, “are continuing to drive nearly 50 percent of application frauds since criminals are finding ways to skirt around even the most sophisticated controls.”

The ease of online account opening makes the creation of “cash repositories” easy and convenient for criminals, adds Eisen. Many times they will use multiple accounts to keep balances from becoming suspicious, he adds. Criminals are also using online applications to create “valid” identities for future activity.

10. Prepaid Cards

The gift card market has always been a target for criminals say, and prepaid cards will continue to be purchased fraudulently with compromised credit cards, says Fair Isaac’s Urban. “The absence of an indicator in the transaction message means a prepaid card purchase cannot be identified during authorization,” he notes. The purchase of prepaid cards with stolen credit cards is an optimal way for criminals to get their hands on what they really want—cash.

Another more recent scam is where criminals will steal prepaid cards from the j-hooks at retail stores, chemically wash off the printed card number, emboss the card with information from a compromised card, and then erase the mag stripe. “They then will use the card and have the cashier key the transaction after the terminal swipe fails,” Urban says.■

Read the complete article online:
http://www.bankinfosecurity.com/articles.php?art_id=2000

ATM Fraud: 7 Growing Threats to Financial Institutions

Skimming, Ram Raids Target Consumers and Their Cash

BY LINDA MCGLASSON

The Heartland Payment Systems (HPY) data breach may be the fraud story of year (so far), but ATM and debit card thefts are growing steadily and frighteningly at financial institutions.

Witness the recent announcement by law enforcement in New York City that a criminal gang had stolen $500,000 from hundreds of customers' bank accounts via skimming devices that read and stored account information at Sovereign Bank branches in Staten Island. The gang installed cameras onto the machines, catching victims typing in their PIN numbers. They also used the information to clone the card information, according to police.

A recent survey by security vendor Actimize shows that almost 70 percent of financial institutions experienced an increase in ATM/debit card fraud claims in 2008 compared to 2007. Twenty-three percent of respondents say those claims jumped by 5 to 9 percent, while the rest noted growth of anywhere between 10 and 74 percent. These numbers are only expected to grow in 2009, as a result of the recession.

Half of the institutions surveyed say they were hit with fraud complaints that came out of some of the major data breaches, with more than 30 percent saying they had seen fraud incidents as a result of the TJX hack, and 30 percent cited the Heartland hack.

> **"Almost 70 percent of financial institutions experienced an increase in ATM/debit card fraud claims in 2008 compared to 2007."**

Approximately 80 percent of the survey respondents say the big data breaches can decrease consumer confidence in ATM/debit card use. About 15 percent say they have reissued cards to more than 20 percent of their cardholder customers. In 2008, the financial institutions surveyed lost an average of $744,321—with some as high as $12 million—to ATM fraud alone, and an average of $145,560, or as high as $1 million, to data breaches.

ATM Fraud Trends

The reason that criminals target ATMs is simple. "Criminals like cards and PINs. It is much easier to cash them out, rather than to hire a mule or repackager with stolen credit cards," says fraud expert Mike Urban, senior director of Fraud Solutions at Fair Isaac. If the magnetic stripe data and pin is available, it is easy money for the criminal to get the cash out of the ATM. "There is no fence, no making an authentic card to use at a retailer," he says. While this crime is much harder to perpetrate, criminals prefer this over other types of credit card fraud, such as signature-based fraud.

Here are the top ATM/debit card fraud trends:

1. Skimming

The upswing in skimming at institutions has caught fraud experts' attention. "A higher percentage of criminals are going straight to a bank and installing a PIN pad overlay and card reader," Urban says. "This is where the transaction goes through, and the customer doesn't realize that their ATM card or debit card has been compromised. I've seen a steady increase over the last couple years on this type of fraud."

2. Ghost ATMs

There are also the "Ghost ATMs," where the entire ATM card reader is blocked off and customers can't perform a transaction. "The customer swipes their card, enters their PIN, and then the fake ATM says it can't complete the transaction," Urban explains. There were several of these types of ghost ATMs that popped up on the east coast back four years ago. One arrest was made in those cases, he notes.

3. Ram Raids

Criminals continue to target ATMs in various ways, with "ram" raids happening more often in the U.S. Ram raids are perpetrated when criminals physically break out ATMs from the wall at the institution. In Texas, the number of ram raids has spurred institutions to partner with law enforcement, and a task force has been formed to fight the raiders. "The opportunity that some non-hardened criminals see is an exterior ATM that can be pulled out, loaded with thousands of dollars," Urban says. "So in terms of crimes of opportunity, people feeling desperate will attempt this crime."

4. PIN ID's

One of the other trends Urban sees happening is where criminals are testing systems to identify PINs. One particular technique is where the criminal captures the magnetic stripe data from a retailer. They then go to an online bank site with a script written on several well known PINs, and run it against the site until they get a match.

> **"In 2008, the financial institutions surveyed lost an average of $744,321—with some as high as $12 million—to ATM fraud alone, and an average of $145,560, or as high as $1 million, to data breaches."**

5. Automated PIN Changes

Another trend Urban sees is criminals go through the financial institution's telephone banking service to change PIN numbers. "They will use the ANI to change

the information on the phone they're calling out from to appear like they are calling from the consumer's phone," Urban notes. If they can find the basic information on the cardholder, name, card account number, last four digits of the social security number, then they're trying to take that information and go to the call center and change the PIN number over the phone. "Thus, while more time-consuming, the overhead cost is cut to near nothing other than their own work to deceive the bank call center," Urban says. Then with the changed PIN, the criminals drain the account. "The easier it is for the consumer to change their account, those are the financial institutions that will be targeted," Urban says.

6. SMS attacks

"Smishing" is the attack that comes through the Short Message Service (SMS) or text venue, onto a smart phone or a cell phone. Urban has personally seen three examples come through recently from institutions that he has no affiliation with, asking him for his account number and PIN. Where the criminals are able to get the information from the customer, they then turn and clone the ATM or debit card and use it to withdraw cash.

"If the magnetic stripe data and pin is available, it is easy money for the criminal to get the cash out of the ATM."

The bank or credit union, if it is not checking for the CVV value, or the full name or expiration date, and just accepts the card transaction, will be hit with counterfeit cards made from data taken in this type of attack. These "smishing" attacks hit several midwest institutions in 2008.

7. Malware

Security researchers say they have found malware code that lets a criminal take control over ATMs. SpiderLabs, the forensics and research arm of TrustWave, found a Trojan family of malware that infected 20 ATMs in Eastern Europe. The researchers warn that the malware may be headed toward U.S. banks and credit unions, as well as other parts of the world. The malware lets criminals take over the ATM to steal data, PINs and cash.

That report from SpiderLabs isn't the only malware found. Sophos researchers in March say they found a Trojan specifically designed to steal information from Diebold ATM users that had infected several ATMs in Russia. SpiderLabs researchers explain the Trojan collects magnetic stripe data and PINs from the Windows XP-based ATM's transaction application's private memory space. Researchers found it came with its own management function that allows the attacker takeover the ATM with a custom interface that may controlled by the attacker when they insert a controller card into the ATM card reader. Both research arms say that they expect the Trojans they discovered to evolve and spread, infecting more ATMs. Trustwave recommends that all financial institutions with ATMs perform analysis to identify if this malware or similar malware is present. ■

Read the complete article online:
http://www.bankinfosecurity.com/articles.php?art_id=2000

ATM skimmers don't just cost you money. They can cost you customers.

Protect them both with new ADT® Anti-Skim™ ATM Solutions.

In a 2009 survey,* a majority of customers polled indicated a strong preference to change financial institutions if they were a victim of ATM skimming. Now you can protect your reputation, your ATMs and your ATM customers—from over $3 billion in ATM fraud losses annually—with ADT Anti-Skim™ ATM Solutions. These advanced technologies:

- Help detect ATM skimming devices and render them useless
- Help protect your cardholders' personal financial information during ATM transactions
- Work on all major ATM makes and models
- Conceal safely within the ATM with no software adjustments
- Bundle seamlessly with ATM alarm/video systems
- Can feature ADT monitoring of skimming alarms

Protect your ATMs today against skimming. Call **1.800.492.2238** to schedule an informative demonstration with your ADT Banking Sales representative or visit **www.ADT.com/banking.**

MONITORING ACCESS CONTROL VIDEO SURVEILLANCE ATM SECURITY INTRUSION DETECTION FIRE & LIFE SAFETY

Top 8 Security Threats of 2010

Financial Institutions Face Risks from Organized Crime, SQL Injection and Other Major Attacks

BY LINDA MCGLASSON

It's a never-ending battle—the list of naughty and downright evil security threats that challenge financial institutions and security professionals. From organized crime to SQL injection, here are the experts' choices of eight major security threats to watch in 2010.

1. Organized Crime Targeting Financial Institutions

Over the past several years, law enforcement investigations into cybercrime have uncovered global networks of organized crime groups, including overseas criminal organizations (many based in Eastern Europe) that hire and direct hackers.

Rob Lee, senior forensics investigator at Mandiant, a risk assessment firm, says the battle between "us and them" increasingly pits the financial services industry against organized crime organizations. "The days of the Maginot line of information security are long gone," Lee says, referring to the defensive World War I battle line created by Allied troops to keep German troops from invading France. The battle lines reach far wider than just an institution's firewalls, he adds.

Anton Chuvakin, an information security expert and author, predicts that 2010 will see a frightening rise in incidents attributable to organized crime. "Rampant, professional cybercrime, from the Russian Business Network (RBN) to its descendants, from individual criminal 'entrepreneurs' to emerging criminal enterprises—all signs point to dramatic rise of cybercrime," he says. "This is simply the logical consequence of today's situation with the use of information systems: Insecure computers plus lots of money plus no punishment equals 'go do it!'"

In other words, there has not been a better time to go into a cybercrime business, Chuvakin says. "The strategy is pretty much the 'blue ocean' one, with a lot of unexplored opportunity and a low barrier to entry."

“From organized crime to SQL injection, here are the experts’ choices of eight major security threats to watch in 2010.”

2. Assault on Authentication

The banking regulatory bodies have long called for mandatory two-factor authentication for all online banking sites. Now industry security experts warn that attacks against those traditional customer authentication methods are being challenged and defeated. Avivah Litan, a Gartner analyst, says the threats include man-in-the-browser attacks that defeat one-time-password authentication from a dedicated token (such as the popular RSA SecurID), and call-forwarding that tops phone-based authentication, as well as transaction verification using SMS or voice calls. “This is bad news for banks that use these authentication techniques to protect high-value accounts and transactions, such as those from business and private banking accounts,” Litan says.

Uri Rivner, head of New Technologies, RSA’s Identity Protection and Verification division, is also seeing an increase in high-grade man-in-the-browser trojan attacks. “In 2009, the emergence of highly customizable, stealthy, MITB-capable trojan kits reached a new height with the introduction of Zeus 2.0,” Rivner says. MITB trojans send money in real time, he explains, rather than just stealing credentials for sale in the underground. Rivner sees additional “Fraud-as-a-Service” models will make these kits available to more and more fraudsters. Solutions include anti-trojan detection and countermeasure services, desktop hardening, out-of-band authentication and transaction monitoring, he says.

Commercial banking has already seen early signs of man-in-the-browser attacks targeting two-factor authentication used to protect U.S. commercial online banking customers. “In 2010, we project this trend to greatly intensify, requiring commercial banks to deploy additional lines of defense such as adaptive authentication, out-of-band authentication, desktop hardening and anti-trojan countermeasure services,” Rivner says.

3. More Malware

It seemed that almost every week in 2009 there was another announcement by a security researcher of a newly discovered malware variant. RSA’s Rivner says malware spread like wildfire. “The rate of the malware infection of personal computers was 10 times higher during 2009 compared to 2008,” he notes. Leading the infection methods are drive-by-download (taking over legitimate websites; routing visitors to an infection server) and social network infections (spamming a victim’s entire social network “friend list” with links to infection servers).

Increasingly, sophisticated, distributed malware is being seen in forensic investigations of cybercrimes, says Dave Shackleford, an information security expert and SANS instructor. Criminals are also adding a flavor of social engineering to get the malware into a user’s machine. “Large scale botnets are growing, and the quality of the code is improving, as these kinds of malware are increasingly funded by criminal organizations,” he warns.

4. Return to Telephone-Based Fraud

One thing criminals attacking financial institutions and customers are is persistent, as seen by the number of attacks hitting U.S. banks and credit unions in 2009. When one avenue of entry is closed, the criminals look to other ways to get what they’re after, says RSA’s Rivner. As institutions beef up their online security, many fraudsters turned to more traditional telephony fraud.

“Armed with data stolen via trojans and phishing attacks—including ‘vishing’ (voice phishing), ‘smishing’ (SMS phishing or text phishing) and variants of spear phishing—fraudsters around the world call customer service departments at banks, credit unions and credit card companies in order to perform fraud called account takeover,” Rivner says. These fraudsters often outsource the actual phone call to multi-lingual third party service providers operating 24/7 out of Russia, he adds. “Caller ID

spoofing is also prevalent," he observes.

5. Increased Insider Threat

The trusted insider is the most dangerous foe for any institution—and the most feared, as seen by the amounts of money and data taken by insiders. The prevalence of insider crime can be blamed on several factors, but the insider threat at financial institutions is increasing, notes Shackleford. "I see there will be an increase in internally-driven fraud, caused in part by the bad economy and also the ease of access to data," he predicts.

Tom Wills, Security and Fraud senior analyst at Javelin Strategy and Research, agrees and adds the insider threat —with the insider defined as anyone with access to the extended enterprise, not only employees and contractors, but partners and suppliers too—may have financial problems that push them toward the crime. "Additionally, you have to consider individuals with significant IT knowledge who may not be fully employed and may have incentive to perform activities that they would not have previously," he notes.

Nathan Johns, a Crowe Horwath consultant, says disgruntled employees may also turn to crime. "These are people who are not receiving raises, bonuses, or potentially being laid off, who have the opportunity to do activities that they would not have done in better times," he observes.

Johns also warns that unauthorized access by former employees can lead to problems. "There has been an increase in people being released by organizations, but often times the removal of their access rights is lagging their departure from the organization," he says.

The employees who become insider threats may do so without even knowing they're involved, warns RSA's Rivner. "Already thousands of Fortune 500, government and bank employees are infected with financial trojans that targeted them as consumers. As a side-effect, there are also thousands of infected corporate laptops or PCs used at home for remote access via a VPN," he warns.

Rivner expects 2010 will see fraudsters developing ways to monetize these infected resources, which can lead them straight into the affected organizations' networks. "Bank employees will be a primary focus for these cybercriminals," Rivner predicts.

6. Mobile Banking Attacks

The move to mobile banking by financial institutions that want to offer customers instantaneous access to their accounts is catching fire around the country, with hundreds of institutions now offering customers the ability to look up their account data and balances on cell phones. But security experts see trouble ahead when institutions begin allowing more than just account balance checks to happen. The chance for fraud via the mobile phone is already here says Ed Skoudis, lead forensic investigator for InGuardians, a security forensic firm. "Exploits against the ever-growing base of smart phones [are on the rise], leading to the possible building of a botnet based on iPhone or Android phones," Skoudis observes.

RSA's Rivner concurs with the propensity for fraud in the mobile banking sector saying, "Mobile banking fraud is coming. More customers are enrolling in mobile banking, and more services are offered via mobile channels. Banks in Asia and Europe are already experiencing mobile trojans and SMS redirection attacks." He expects the U.S. to experience the first wave of attacks towards middle of 2010. "Banks will start funding the extension of their online banking protection to the mobile channel," he predicts.

Part of the problem is that customers don't always pay attention to what they're receiving on their mobile devices, says Johns of Crowe Horwath. "People rely more and more on their BlackBerrys and smart phones, and don't pay attention to the information that they are getting on them, and they push back to security being installed on the devices," he adds.

Javelin's Wills sees mobile fraud happening if banks start to enable full service banking on mobile devices. "This means money movement instead of just checking balances and finding ATM locations," he says.

The mobile target will continue to grow, says Shackleford, and as smart phones become more sophisticated, the number of attacks will grow too. "In many cases, these devices contain a huge amount of sensitive data, as well, and could even be a vital component of newer two-factor authentication used by banks," he says.

7. Web 2.0 and Social Media Attacks

At the same time institutions are flocking to Facebook and tweeting on Twitter, the cybercriminals are lining up their arsenals for attack via Web 2.0 and social media sites. InGuardians' Skoudis says attacks via social networking sites are the new way for criminals to get into bank accounts. "These sites are being used by the bad guys for reconnaissance to learn more about their targets," says Skoudis adding, "At the same time, they're delivering malicious content to unsuspecting users."

Institutions should also be on lookout for additional client-side spear phishing attacks which will expand into new means of targeting users through use of social networks says Lee of Mandiant.

8. SQL Attacks—More To Come

The biggest data breach on record—Heartland Payment Systems—was done using a "Sequel Injection," or SQL injection, attack. SQL attacks are a popular way to infect and take over websites, as seen by the recent findings by security researchers at Verizon Business. SQL injection attacks were one of the most common methods of breaching systems in the Verizon report's cases. They were used in 19 percent of the cases and accounted for 79 percent of the breached records.

There's more to watch for, says Javelin's Wills, including attacks on web applications—especially drive-by downloads of keylogging trojans and man-in-the-middle attacks. The browser will become the favored attack vector, and zero day attacks on client-side software are also on horizon.

"Fewer operating system holes are being found, but more and more in Adobe, instant messaging, MS Office and other applications," says InGuardians' Skoudis. "The scenario would be: A victim views content from a bad guy, and the attacker then takes over the victim's browser," he explains. This technique is used to create botnets as well as skim credit card and account information from the client machine.

He also sees infrastructure attacks, launched via an infected browser happening. "Here, the bad guy uses a compromised browser to access an enterprise infrastructure controlled by that browser including the enterprise's firewalls, anti-malware solution and possibly HVAC and related systems," Skoudis says.

Within institutions, Shackleford sees VoIP and other converged networking issues coming up "From simple denial-of-service problems to new malware that affects voice systems, this will be a growing area that affects financial institutions," he predicts. ■

Read the complete article online:
http://www.bankinfosecurity.com/articles.php?art_id=2019

Gartner’s John Pescatore on 2010 Threats, Trends

Malware, Consumer Technology, Social Networks Head the List of Vulnerabilities

Listen to this interview online >

BY TOM FIELD

Know what scares security expert John Pescatore the most? The image of a remote employee sitting at a home office or public setting, plugging into an unsecured network, accessing critical business data via a personal laptop or PDA.

Organizations have never had so many security risks in so many remote locations, says Pescatore, vice president and distinguished analyst with Gartner, Inc. Mitigating these risks will be among the primary challenges for information security leaders in 2010. In a discussion of security trends, Pescatore offers insight on:

- Emerging threats;
- Emerging solutions;
- The role of education and training to help meet security needs.

Pescatore has 31 years of experience in computer, network and information security.

Prior to joining Gartner, he was senior consultant for Entrust Technologies and Trusted Information Systems, where he started and managed security consulting groups. His previous experience includes 11 years with GTE, as well as employment with NSA and the U.S. Secret Service.

John Pescatore

TOM FIELD: Now, John, everybody from the president on down this year is talking about cybersecurity. What do you see is the top information security issues that face businesses and government agencies as we head into the New Year?

JOHN PESCATORE: Well, I think there are new challenges and there are some continually old challenges. I mean, one consistent question or message we get from chief information security officers is around security metrics

“I would like to see an emphasis on getting to students earlier in their careers — even to hit them in high school, not as part of this program”

and trying to answer the CEO or the CIO question, “Are we safe?” You know, that is still a very hard question to answer. It’s hard to express that in business terms. There have been a lot of tries just treating security like you would treat other business risks like financial risk, and that hasn’t worked.

So I think one major challenge continues for CISO’s is just demonstrating the value of the cybersecurity or information security program, but also trying to give a dashboard look at “Are we safe? Are there problems coming? Are we spending too much or too little?” Now that is a continuing problem.

However, there are two very new challenges. What we’re seeing happening right now is certainly the threats have changed, but also business processes and the demands put on the IT organization and the information security organization are changing. At the same time that threats are getting more targeted, the business, even government agencies, are demanding that users be allowed to use home PC’s, their own smart phones, iPhones and the like, being allowed to work from home, being allowed to use social networks, use consumer grade things like Google apps and Skype and the like.

So at the same time that the threats are getting more focused, IT is being forced to relinquish some control over the hardware and software and services that users use to get the business done and touch privacy related information and critical business processes. So dealing with those two challenges simultaneously, we’re targeting deeper threats and having to give up some levels of control. That, I believe, is the major challenge facing security programs today. ■

Read the complete interview transcript online:
http://www.bankinfosecurity.com/articles.php?art_id=1926

Think You Have Check Fraud Covered? Think Again.

Why Conventional Wisdom May be Wrong

BY TIMOTHY T. LI, DEPOSIT RISK MANAGER, JPMORGAN CHASE AND MICHAEL MULHOLAND, DIRECTOR, FRAUD SOLUTIONS STRATEGY, MEMENTO

With the current economic uncertainty, the motivation for committing check fraud is higher than ever. Fraudsters have more information (personal, account, and more) than ever at their fingertips. Organized crime rings are hatching more sophisticated schemes resulting in higher losses. And fraud has never been more intertwined across channels, borders, and more. It's no wonder that check fraud, which hits one of the widest used payment mechanisms, is on the rise. The real question is – have you really done everything you can to control it?

Banks and credit unions of all sizes are asking themselves the question again. Their answer? We're doing more. "Our overall strategy is to try to reduce fraud by 25 percent," says one senior executive with a mid-sized regional bank. "We're seeing fraud that's increasingly sophisticated and that combines multiple channels. We're seeing more check fraud, and becoming more aware of how it can be categorized as something else. And we're responding by aggressively working to stop it – from trying to detect fraud more proactively and intuitively to working to reduce false positives to providing more training at the branch level."

Here we take a look at three common misconceptions about check fraud management:

Michael Mulholand

Timothy T. Li

"We've got check fraud under control."

That's what we hear from some of our colleagues. But what does it really mean? It's important to know that the real cost of fighting check fraud involves fraud losses plus the cost of preventing check fraud. This cost can include the cost of people and processes, not just technology. If you've invested heavily in teams of analysts, and their days are filled with sorting through a flood of false positives from simple, rules-based systems, then you may be paying far too much to stop fraud.

A more accurate, automated fraud detection solution requires investment, but can help drive this cost down, particularly if it can rank alerts to make analysts more productive by focusing them on the highest-risk cases. And equally important, any system should include a closed feedback loop that enables the system to learn from real-world outcomes.

"Our check fraud losses are within our expected loss range, so we're OK."

Check fraud is sometimes considered a cost of doing business. But how much of a cost, and is it being measured correctly? Check fraud may be one of the oldest types of fraud, but it's also one of the most poorly categorized. A check fraud related loss may be classified as a return, an overdraft, or simply an operational loss. No matter how it is categorized, banks need to count up all the ways that they are affected by check fraud. Many have totaled the damage, only to find that it is usually the single biggest category of fraud loss, and a category for which they are able to consider a solution upgrade.

"Sure, check fraud is a problem, but we want an enterprise fraud solution."

Approaching fraud from an enterprise perspective is the right approach. And, of course, check fraud doesn't exist in a vacuum. It's part of the overall fraud continuum, from online to wire to credit card to debit and beyond. After all, fraudsters don't differentiate between channels the way financial institutions do. They're simply trying to get to the money in any way that they can. A rise in overall fraud triggers an increase in check fraud. Access to new information via online and other electronic channels opens up new opportunities for committing check fraud.

But solving check fraud now – a fraud category that banks understand well, and take big losses in – can be the right first step towards an enterprise fraud solution. And justifying an investment in check fraud can be easier.

Since you likely have personnel and processes in place for addressing check fraud (even if inefficiently deployed) the cost of fighting the problem makes it a great starting point for improving your overall enterprise fraud management program. The savings you gain from upgrading your approach and putting the lid on check fraud can be applied to addressing emerging fraud types that are likely to hit in the future, but that haven't yet cracked your list of top loss areas.

As fraud becomes more of a cross-channel problem, you can be sure that check fraud will be part of it. And while consumers (and the financial institutions that serve them) may tend to be focused on the more publicized threats of identity fraud and other types of online fraud, ultimately, these types of fraud reinvigorate check fraud as well.

To banks that think they have check fraud covered, the banking executive with whom we spoke offers this advice. "There are more and more opportunities where fraud can occur," she says. "Check fraud is getting worse because fraud is getting worse. Anyone who thinks they've got check fraud covered needs to take a careful look at whether it's really working – and how much it's really costing." ■

Timothy T. Li and Mike Mulholand were co-presenters of "It's On Us to Stop Check Fraud" at the recent BAI Combating Payments Fraud conference at BAI Payments Connect.

2010: A Good Time to Start an Information Security Career

With the global recession barely in the rearview mirror, you hear a lot of people saying one of two things: “I’m lucky to even have a job” or “This is a lousy time to be looking for work.”

BY TOM FIELD

I hear that latter statement, especially, and think to myself “Man, not if you’re in information security!”

For a lot of reasons, now is a very good time to be looking for work if your talent is protecting other people’s data.

First of all, from the president on down, this nation is all about cybersecurity these days. It’s one of the three hottest topics in Washington, D.C., and as my colleague Eric Chabrow says, you’re likely to see some major cybersecurity policy at least discussed in 2010. Government agencies are eager to hire new, skilled security professionals.

The second hot topic in D.C. is healthcare. In 2009, the federal government gave healthcare organizations a boatload of money to create electronic records, and in 2010 it’s going to enforce new regulations to help protect those records. Think this initiative won’t call for additional personnel skilled in risk management, privacy and incident response? Good time to be an information security professional in healthcare. And stay tuned, please, for further discussion on this subject.

And then there’s banking reform—the third hot topic in D.C. And while it’s hard to imagine exactly how the regulatory agencies will be reshuffled when all the dealing is done, it is clear that: 1) There will be increased regulation, especially for non-banking financial institutions; 2) There will be greater consumer advocacy and security standards; 3) All of this regulatory pressure is going to require new bodies inside the institutions to secure critical systems, as well as outside to examine them.

Like I said, a good time to either start or re-start a career in information security.

I caught up recently with David Foote of Foote Partners LLC, a leading IT staffing research firm. He’s been tracking technology-related job trends literally for decades now, and his assertion flat-out is: There’s never been a better time to be an information security professional. “This year and next year, bar none, security is the smart place to be in IT,” says Foote, who in his conversation with me discusses the wave that has driven the surge in security jobs, as well as his predictions for 2010-2012.

I’d be remiss if I didn’t mention our recent Information Security Today Career Trends Survey, which looks at academic, business and industry objectives for 2010, pointing to risk management, cybersecurity and fraud/forensics as the hottest topics for training in growth.

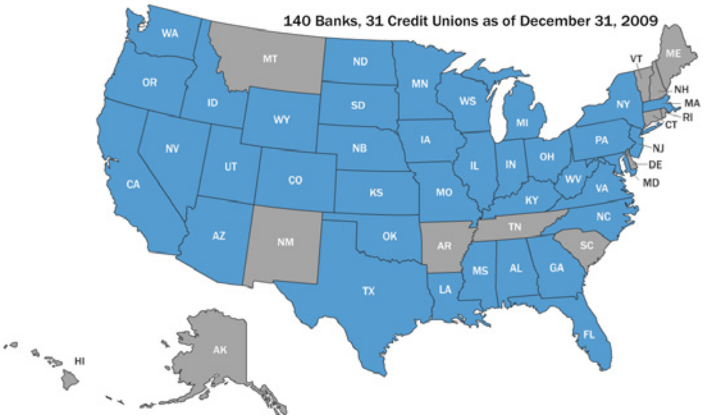
But what’s the career outlook from your perspective? Where do you see the best information security jobs in 2010, and what are you doing to grow your own career?

Here’s to a prosperous—and secure—2010. ■

Read the full blog post online:
http://blogs.bankinfosecurity.com/posts.php?postID=411

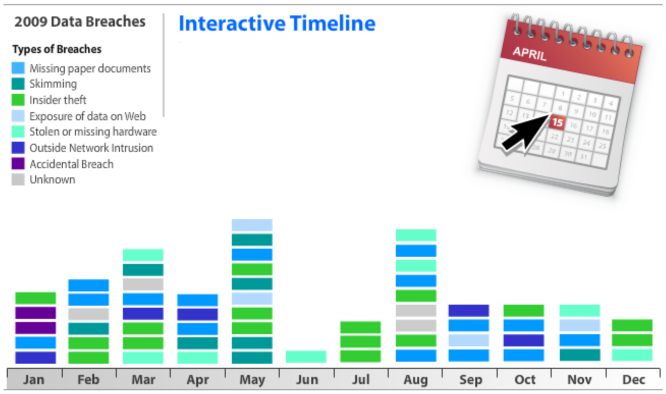
Failed Banks and Credit Unions, 2009 Data Breaches

See Exactly Where Institutions Were Closed or Acquired in 2009



View the map online at
http://www.bankinfosecurity.com/articles.php?art_id=1681

A Look at the Top Breaches Involving U.S. Financial Institutions



Read the complete list online at
http://www.bankinfosecurity.com/articles.php?art_id=1766

BANKINFO SECURITY®

Just for Credit Unions
CUINFO SECURITY®

GOVINFO SECURITY®

HEALTHCAREINFO SECURITY®

iSMG
INFORMATION SECURITY
MEDIA GROUP

4 Independence Way | Princeton, NJ 08540
ISMGCorp.com