

## 10 Faces of Fraud for 2010

*Ghosts of Crimes Past and Present Will Haunt the Future*

By Linda McGlasson, Managing Editor of BankInfoSecurity.com

December 14, 2009 - "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.

[www.executivebank.com](http://www.executivebank.com) | 305.274.8382



**MAIN OFFICE**  
9600 North Kendall Dr.  
Miami, FL 33176

**AVENTURA**  
20900 NE 30<sup>th</sup> Ave.  
Aventura, FL 33180

**DORAL**  
8009 N.W. 36<sup>th</sup> St.  
Miami, FL 33166

**SOUTH MIAMI**  
7220 Red Road  
Miami, FL 33143

**TAMIAMI**  
13354 SW 128<sup>th</sup> St.  
Miami, FL 33186



### 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.

Fair Isaac's Urban sees this as "first-party fraud," where criminals create accounts and build credibility as a customer with a financial institution, and then "bust out" the accounts once they are fully leveraged. And it may spill over to financially pressured consumers, "who may get caught up in this type fraud with high unemployment and benefits starting to run out," Urban 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.

There is a increased level of sophistication being seen in the phishing attacks, says Ori Eisen, former worldwide fraud director for American Express, now head of 41st Parameter, a fraud solution company. Eisen sees increased sophistication in phishing and use of SMSing attacks, similar to the **text phishing attacks** that have been circulating around the country, hitting banks and credit unions.

[www.executivebank.com](http://www.executivebank.com) | 305.274.8382



**MAIN OFFICE**  
9600 North Kendall Dr.  
Miami, FL 33176

**AVENTURA**  
20900 NE 30<sup>th</sup> Ave.  
Aventura, FL 33180

**DORAL**  
8009 N.W. 36<sup>th</sup> St.  
Miami, FL 33166

**SOUTH MIAMI**  
7220 Red Road  
Miami, FL 33143

**TAMIAMI**  
13354 SW 128<sup>th</sup> St.  
Miami, FL 33186



"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 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 diligent monitoring their accounts or come in looking to withdraw the money from those accounts.

[www.executivebank.com](http://www.executivebank.com) | 305.274.8382



**MAIN OFFICE**  
9600 North Kendall Dr.  
Miami, FL 33176

**AVENTURA**  
20900 NE 30<sup>th</sup> Ave.  
Aventura, FL 33180

**DORAL**  
8009 N.W. 36<sup>th</sup> St.  
Miami, FL 33166

**SOUTH MIAMI**  
7220 Red Road  
Miami, FL 33143

**TAMIAMI**  
13354 SW 128<sup>th</sup> St.  
Miami, FL 33186



## 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 are 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 the 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.

[www.executivebank.com](http://www.executivebank.com) | 305.274.8382



**MAIN OFFICE**  
9600 North Kendall Dr.  
Miami, FL 33176

**AVENTURA**  
20900 NE 30<sup>th</sup> Ave.  
Aventura, FL 33180

**DORAL**  
8009 N.W. 36<sup>th</sup> St.  
Miami, FL 33166

**SOUTH MIAMI**  
7220 Red Road  
Miami, FL 33143

**TAMIAMI**  
13354 SW 128<sup>th</sup> St.  
Miami, FL 33186

