



learn self-defense.  
learn system defense. [easyeasier.com](http://easyeasier.com)

Microsoft®  
**Forefront™**

Mic



## Fraud Techniques Evolve in Parallel with Bank Products and Defenses

May 05, 2007

URL: <http://www.banktech.com/showArticle.jhtml?articleID=199203702>

Fraud likely has been around in some form for as long as people have been using banking services. But while the crimes remain a constant for financial institutions, the methods for perpetrating them have become just as diverse as the products and services offered by banks. Today's financial institutions have to be on their toes more than ever to keep that one important step ahead of fraudsters.

This isn't easy in a world where fraud has become the domain of organized crime rings with vast resources that often are out of reach of domestic law enforcement. "We're seeing an increase in losses across all fraud types in the context of fraud rings being more organized and sophisticated with their use of technology," says Christopher Ward, SVP and manager, payables and receivables solutions, with Charlotte, N.C.-based [Wachovia](#) (\$707 billion in assets). "But [banks'] ability to detect and stop losses is growing faster than the losses themselves."

"The bad guys are more ingenious today," adds Milton Santiago, SVP, head of electronic banking products, for [ABN AMRO](#) (Amsterdam; US\$1.3 trillion in assets) in Chicago. "For example, in traditional check fraud, they'd wash the entire check and alter all the information on it. Once positive pay was introduced, criminals got wise to this and just modified the payee information. So banks responded and developed payee positive pay."

The tit-for-tat dance goes on. As the fraudsters' techniques evolve alongside the products and services offered by financial institutions, new steps must be introduced to stop them. "The overall mix of fraud is changing — it's becoming more diverse," observes Jerry Cranney, SVP in the client services group at Cleveland-based [KeyBank](#) (\$92 billion in assets). "Fraudsters are utilizing more tools and systems to commit fraud. We're in a world where fraud is perpetrated by check but the criminal uses ACH or wire transfer to actually move the funds more quickly. So it's more of a challenge for banks to recover the funds."

### Cross-Channel Fraud

In essence, banks aren't the only ones to employ a multichannel strategy, according to Fair Isaac's (Minneapolis) William Ferguson, senior director, [enterprise fraud solutions](#). "Now fraud is becoming more cross-channel," he explains. "They'll phish a customer's information online and bring up an image of a check where they can get a picture of the signature and see the check number to commit the fraud."

David Luther, VP of the global financial services practice at [Unisys](#) (Blue Bell, Pa.), says he also sees evidence of cross-channel fraud, particularly in deposits. "Check deposit fraud seems to be of most concern to my clients," he says. "Fraudsters are finding new ways to attack this channel. They can forge checks better. So they'll deposit a fraudulent check and use another channel, like a debit card at a gas station pump, to perform

small transactions to see where the funds are. They're using multiple channels to commit fraud today."

"[Fraudsters] are coming at it from all angles," agrees Wachovia's Ward.

In addition to responding to heightened threats, banks now must be more vigilant in their anti-fraud measures than ever before given the tougher regulatory environment. In a post-9/11 world, the stakes have been raised for financial institutions in a number of areas, particularly in anti-money laundering (AML). With [Office of Foreign Asset Control](#) (OFAC) checks and suspicious activity reports, banks have their hands full staying compliant.

According to KeyBank's Cranney, the bank invested a great deal of time and money in AML. After all, he states, "You cannot afford to have a compliance problem here."

But fraud prevention today is about much more than simply staying compliant, according to Tim Paydos, director of [threat and fraud intelligence](#), IBM (Armonk, N.Y.). "More recently, the challenge in banking is that fraud is going beyond regulatory compliance to reputational risk and customer loyalty issues," says Paydos. "There's intense fraud pressure pushing things to the tipping point, so fraud is more top-of-mind with senior line-of-business executives today at banks."

James van Dyke, founder and principal of [Javelin Strategy & Research](#) (Pleasanton, Calif.), says he applies a three-pronged model when examining banks' anti-fraud efforts: prevention, detection and resolution. Javelin issues a scorecard with which it compares banks on these measures, he notes.

"Over the last three years, we've seen some changes. Historically, banks focused on fraud resolution first," van Dyke says. "They were very low on prevention and detection. But as the years went on, detection increased at banks. This year we called for an improvement in prevention, [but] I haven't seen this much yet." Prevention measures, he explains, can be things as simple as not issuing paper statements to actually involving customers in the fraud-prevention battle by allowing them to set parameters and thresholds for when they should be alerted to suspicious account activity.

After all, points out Arlene Chapman, senior consultant, technical services, the [Association of Financial Professionals](#) (Washington, D.C.), you want to prevent the fraud from entering the system in the first place.

## **A Diverse Anti-Fraud Toolbox**

The tools banks use in their battle with fraudsters are diverse. Although none of the banks interviewed for this article were at liberty to name their specific solutions, they were able to offer an idea of the functionality of their anti-fraud systems.

In spite of findings to the contrary by Javelin, many banks — including Columbus, Ohio-based [Huntington Bancshares](#) (\$36 billion in assets) — are trying to beef up their prevention efforts. According to Dick Harp, Huntington's SVP and director of corporate security, the banks' primary focus today is on prevention. "There are a number of tools available that can predict or identify suspicious activity so you can shut an account down and prevent the fraud," he says. "We have a tool that monitors debit card activity — it identifies suspicious card authorizations and multiple transactions within a set period of time. We have a tool that monitors checks issued against Huntington accounts to see if the check numbers are out of range, for example. We also have a rules-based system to identify deposits to see if any data is out of the ordinary."

These tools are used in addition to systems used in the actual account-opening process that can compare and verify specific pieces of information provided by the customer, according to Harp. Further, Huntington provides customers with access to the [Identity Theft Assistance Center](#), an initiative spearheaded by [BITS](#) to help people who have fallen victim to identity theft.

ABN AMRO's Santiago says his bank has been implementing more technology on the back end to identify

fraudulent transactions, especially since it began offering online banking services in the '90s. Many of these tools have been developed in-house, he notes. On the commercial side, clients are required to use a hardware token to initiate ACH payments, Santiago relates, adding that they can also set thresholds to communicate to the bank whether a transaction amount is permitted. In addition, the bank also employs authentication technology at login that prompts clients for credentials using dual-factor authentication.

"The system also has the capability to detect where you're accessing our site from -- we're enabling the site to understand the machine the customer is using," Santiago explains. "If they're using a different computer, they're prompted for more credentials. This makes your computer part of your identity."

However, "Fraud protection comes in multiple forms, [and] one of the strongest ways to combat fraud is through education," Santiago adds. "This is our first weapon. When we onboard clients, we educate them on our best practices for how we communicate with them. When new scams arise, we post warnings on our Web site for our clients, too."

Phillip Upton, a principal with PricewaterhouseCoopers (New York), says there are multiple layers to a fraud prevention strategy, including transaction monitoring, risk scoring and item investigation. "This technology has been around for a while, but it's prone to false positives," he says. "Banks need to improve the investigation process. However, whatever system is used to identify items for investigation, someone has to examine the evidence to determine whether it's fraudulent. Refining this investigative process will enhance efficiency and improve the accuracy of the result. Getting this part right should increase the coverage of the alerts being generated by monitoring systems and decrease the hours spent analyzing items."

### **An Enterprise View of Fraud**

However, Upton concedes, not many banks are at a point where they can obtain a single view of fraud activity across the enterprise because it requires the ability to draw data from different systems into one dashboard. While the technology to aggregate disparate channels and data stores is relatively new, however, a services-oriented architecture can help banks tap into their legacy systems and unlock information stored in disparate systems, he notes.

The idea of pooling data throughout the bank to gain a single enterprisewide view of fraud is where many in the industry believe fraud prevention needs to go. Once again, siloed operating environments are preventing financial institutions from gaining real efficiencies. "It's counterproductive to have independent entities," says Huntington's Harp. "You have to blend what you do with other areas. You can't live in a silo and be effective in combating fraud."

Fair Isaac's Ferguson says silos remain a struggle for banks today. "It's to the point where in some banks, even a debit card has responsibility in two different fraud groups -- one for the PIN side and one for the signature side," he laments. "Banks need the ability to do analysis across silos and see all the activity of the customer with all the channels interlinked."

"Silos are definitely hindering financial institutions in terms of not being able to manage fraud holistically," says Derren Jones, director of product management, fraud and risk with ACI Worldwide, an Omaha, Neb.-based provider of electronic payments solutions. "If I monitor a customer on just his credit card transactions, that doesn't tell me much."

These are the same arguments used on the customer relationship management side for bringing together various databases from the lines of businesses within a bank, Jones notes. In fact, when he worked in the fraud department at a major Australian bank, Jones says, his unit and the CRM unit there often collaborated with one another. "The fraud database and the CRM database are basically the same."

It is perhaps for this reason that PwC's Upton prefers to refer to this concept as a customer-centric approach to fraud, rather than an enterprisewide approach. "It's about customer-centricity, not the account-centric approach

most banks take," he explains. "If you take an account approach to fraud, you may not fully appreciate the customer's true relationship with the bank. You want to look at the totality of the customer's interactions with you."

The AFP's Chapman says the organization has been urging banks to link their check and ACH systems to each other for years. "If they do this, they can catch a fraudulent check transaction when it's submitted as an ACH. In our [survey](#), only 14 percent of [corporate] respondents reporting ACH fraud said their banks linked the two systems."

Vital to bringing these elements together is the data. For too long, IBM's Paydos says, banks' fraud departments have been operating in a query state. This limits their prediction strategies. "Banks take a data-warehouse approach to fraud," he explains. "They extract the information and then analyze it. This is untimely and after the fact. The longer the data is out of the system, the more inaccurate it gets. Banks are starting to drive fraud intelligence at the operational level. They want the system to be smart enough to give them answers."

"Assessing what the data means and being able to plan and prepare and act quickly on your feet are key" to combating fraud, states KeyBank's Cranney. Therefore, "The infrastructure that backs up your fraud efforts is important."

### **Teaming Up to Fight Fraud**

Some are even looking beyond the enterprise to combat fraud. At Wachovia, in addition to its own in-house fraud systems, the bank is engaged in a collaborative fraud prevention effort with other financial institutions. Early Warning Systems, which is jointly owned by a number of banks -- including Wachovia, Bank of America, JPMorgan Chase and Wells Fargo -- is designed to pool best practices in fraud prevention on a cross-institution basis. "Early Warning Systems is a trusted third party where we collaborate on our fraud activities, share best practices, and develop technologies and solutions all of us can use," Wachovia's Ward explains.

Such cooperation is something Danne Buchanan, CEO of [NetDeposit](#) (Salt Lake City), a subsidiary of Zions Bancorporation that provides check processing solutions, says he would like to see more of going forward. "A good bank looks at fraud and risk throughout its four walls," he says. "But I wish banks would also look at fraud across institutions."

"You need a departmental strategy, a payment system strategy, an enterprise strategy and an industry strategy to manage fraud systematically," says Wachovia's Ward. "You wouldn't want to keep this information proprietary."

"Fraud's going to happen," warns ABN Amro's Santiago. "So what do you do to protect yourself? You need the right tools and good education. As long as you recognize what's real, valid and recurring, anything else will stand out [as fraud]."

**For more information, read:**

#### **2007 BANK TECH FORECAST**

[TowerGroup Predicts A Big Year For Fraud Detection](#)

#### **2007 EARLY WARNING SERVICES**

[Financial Services Firms Join Together To Fight Fraud](#)

[To Improve Security, Businesses Increasingly Are Using ACH Payments With UPICs](#)



[Copyright © 2004/5 CMP Media, LLC](#) | [Privacy Statement](#)