

MOBILE MADE EASY

# usBanker

December 2010

[us-banker.com](http://us-banker.com)



## Brainstorm

Small institutions are developing creative strategies to overcome big industry challenges. Here are nine of the best.



## Inside Jobs

Large and small banks alike are dealing with a spike in fraud, much of it by trusted employees **By Katie Kuehner-Hebert**

### **Wells Fargo investigators had the crime mapped out.**

Using computer logs and IP address-tracking software, forensic auditors at the bank found the digital fingerprints of an employee suspected of fraudulently transferring a large amount of money from a wealthy customer's account. A second account used to transfer the funds listed the employee's home address, and a log-in trail proved the account was created from her workstation with her credentials.

But it wasn't enough to ensure that the case would stand up to legal scrutiny.

"One of the problems is that, while I can pinpoint the computer, I cannot always determine who was sitting there," says Jeff Maw, a computer crimes and forensic investigator for Wells.

So his job was only partly done despite the seemingly strong evidence. The example shows how deep and involved forensic auditing has to be when examining possible fraud. Part of the challenge is to figure out what information is necessary to make a case, and another part is to gather that information without anyone catching on. The secrecy is to avoid inadvertently jeopardizing a case being built against what may be an ongoing crime.

Wells and other large banks have internal forensic teams with the expertise to tackle an anticipated spike in crime. But few small banks can afford to have investigators on staff and many turn to outside specialists for help.

This trend is expected to become even more prevalent as bank fraud continues to rise. For internal fraud alone, the number of investigations at banks and other financial services firms conducted by certified fraud examiners more than doubled during 2008 and 2009 from the prior two-year period, to 298, with a median dollar loss of \$175,000 to the institutions, according to the Association of Certified Fraud Examiners.

Banking companies report more cases of fraud to the association than companies in any other industry, accounting for more than 16 percent of the total this year.

Though forensic investigation at banks is nothing new, the increasing sophistication of crimes, coupled with an economic backdrop that is driving up the number of fraud

attempts, make it even more challenging to protect customers, says Wells' investigations manager Sandi Holland.

"Criminal elements are targeting smaller companies who may not have, nor can afford, a high-tech information security program to protect their network and consumer data against malware written to steal credit and debit card data from unsuspecting victims," Holland says. "This has created a need for cutting-edge investigative techniques and timely response."

Criminals from outside a bank aren't the only ones using the latest high-tech schemes; bank employees are also becoming more technically advanced in perpetrating fraud, as illustrated by Wells' recent case.

In that investigation, Maw and Holland initially hit a dead end in terms of proving that the bank employee had ripped off the wealthy customer. So they dug into data the bank collects through its voice response unit.

Maw determined that a cell phone had been used to validate the amount of trial deposits the bank put into the customer's account, which gave authorization to access the account. The cell phone number was listed on the employee's personnel file, and Maw says that it had been used to gain access to multiple customer accounts, all of which had physical documents that flowed through that employee's workstation.

When Maw's team found the cell phone in her possession—along with additional data from her fraud victims—it was enough evidence for the police to make an arrest. She has been fired and is awaiting prosecution.

"This case is a great example of the complexities that forensic investigators like us work through every day," Maw says. "It requires attention to detail and plenty of intuitive detective work to get a case from the computer to the courtroom."

Agile Risk Management in Tampa,

Fla., is one of the firms that works with small banks to investigate fraud. Matthew Shannon, an Agile principal, says the firm also created F-Response, a forensic software tool used to remotely review data from suspects' personal computers, cell phones and other devices.

"The single most challenging piece is getting to the data," Shannon says. Executives often have the most crucial information on a laptop, and "they are pretty sharp cookies, so taking it from them sets off alarms."

F-Response can prevent users from altering or erasing evidence. And because the tool doesn't tamper with data—just allows for reading it—the evidence tends to hold up well in court, Shannon says.

Banks also must be careful they aren't actually doing things that impede the investigation and stymie prosecution.

For example, a bank may terminate an employee suspected of fraud, but then forget to take their laptop and cell phone out of circulation. So then the information technology staff cleans out the data stored in the equipment in order to reissue it to other employees.

"This can be a real problem because once something is wiped and recirculated, it can be more difficult to recover information, or makes whatever is recovered become suspect," Shannon says. "A good defense attorney can get evidence thrown out."

Looking outside for assistance isn't exclusive to small banks. Even large and midsize banks with their own internal forensic teams bring in help sometimes, says Mari Reidy, a partner in the fraud and ethics practice of Crowe Horwath in Chicago.

"They feel that it's necessary to bring in assistance from a service provider that is completely independent from the bank," Reidy says. "They know this could have some type of negative PR impact on their customers, so they want their customers to be assured they had

done everything possible to rectify the situation."

Employees are often the culprits when fraud occurs, and outside investigators, with the benefit of being objective, can be more effective at catching these suspects than coworkers, Reidy says. "They don't want to believe someone they've trusted all these years perpetuated these schemes."

Three of Crowe Horwath's recent cases at banks involved trusted longtime employees who historically were not questioned about their activities. All three had opened accounts and transferred money from customers' accounts or lines of credit. To help avoid detection they redirected monthly account statements to themselves.

In two of the cases, the employees maintained a separate ledger of the hijacked accounts and provided customers with doctored statements after temporarily altering the accounts to reflect bogus balances. Those ledgers were key to solving the crimes, Reidy says.

When internal controls are weak, as was the case at these three banks, the chances of other fraud schemes, perpetrated by other employees, go way up. Of course, once any fraud is uncovered, scrutiny also increases. "I think the banks who were involved are now taking more seriously the importance of scrutinizing controls and looking for weaknesses by doing such things as running reports every month to find out which customer statements are being held and why," Reidy says.

## POWERFUL, FLEXIBLE SERVICING SOLUTIONS.

### LENDER PROCESSING SERVICES.

Consumer lending faces unprecedented challenges in today's evolving marketplace. You need a comprehensive solution to manage compliance, mitigate risk and enhance your customers' experience. Stay ahead of the competition and **LOOK BEYOND with LPS'** single-servicing solution for all your consumer lending products.

- Traditional mortgages
- Home equity loans and lines
- Direct auto loans
- Secured and unsecured loans

Contact LPS today at **800.991.1274** or visit [www.LPSVCS.com](http://www.LPSVCS.com) to learn more about the technology and services for today and tomorrow.



# LOOK BEYOND.

ORIGINATION | SERVICING | RISK MANAGEMENT | DEFAULT



800.991.1274 • [www.LPSVCS.com](http://www.LPSVCS.com)