

All fraud, all the time

Lately it seems that fraud is top of mind in all sorts of areas where banks are concerned. Just in the past few weeks various observers have raised red flags. For example:

- **Cloud computing security:** Trend Micro says the percentage of companies that reported a data security lapse or issue with their cloud service is approaching half, increasing from 43% in 2011 to 46% in 2012. Over half of the companies say data security is a key reason for holding back their adoption of cloud solutions.

"Cloud computing is a reality for all enterprises operating today. However, in the race to put data in the cloud to save on overall costs, companies need to be aware of the hidden cost in terms of data security," says Dave Asprey, vice president of cloud security, Trend Micro.

- **Credit and debit card fraud:** In its analysis of losses for credit cards from January 2010 to September 2011, FICO found that card-not-present fraud losses increased at twice the rate of counterfeit card losses. Meanwhile, as debit card use has increased 15% over that period, fraud techniques such as skimming has also increased.

"More online shopping has created a shift towards more online fraud, which is proving to be a popular, relatively safe, and anonymous means for fraudsters to exploit any weakness in fraud systems," says Doug Clare, vice president of Product Management at FICO. Consumers and issuers should also remain diligent when using cards for point of sale and ATM transactions, he says.

- **Mortgage and savings fraud:** The mortgage industry saw a 23% jump in attempted fraud rates between April and June 2012, says Experian. Savings accounts saw a 109% rise in fraud rates over the period.

"Over the course of the last year, we have seen mortgages continue to be targeted at a high rate, with more people trying to misrepresent their personal, employment, and credit information on applications to get properties out of their reach," says Nick Mothershaw, director of Identity and Fraud Services at Experian.

(Not to mention, of course, is the ongoing threat of check fraud, which Fiserv's Mile Urban talks about in a Tech Topics interview elsewhere in this issue.)

That's all worrisome enough. On top of it, though, is the indication that bank customers hold their bank responsible for recompensing them for the fraud—even though, as is implied in the above examples, the users and consumers bear at least some or equal responsibility.

Remember the Guardian Analytics survey in Tech Topics a couple of issues ago? It found that 72% of small businesses hold their financial institution primarily accountable for ensuring that their online bank account is secure, while only 43% say their financial institution takes appropriate action to limit risky transactions. Even more scary, 56% say it would take only one successful fraud attack to lose confidence in their financial institution's ability to provide adequate security.

"This year's data confirms that small and medium-sized businesses are looking to their financial institution to be the expert on fraud prevention, and they have every right to do so," says Larry Ponemon, chairman and founder of Ponemon Institute, which conducted the survey.

It doesn't help that more than half of the IT administrators at small businesses would not bet their own money that all of the computers their business owns and employees use are free of malware, according to a recent study by GFI Software.

So what's the answer for banks? FICO points to enterprise fraud management, which basically makes use of analytics of Big Data and coordinates it across all channels.

FICO says in a recent white paper (accessible in the link below) that the banking industry is moving away from the pursuit of a monolithic system that displaces existing fraud initiatives. In its place, it calls for a combination of existing and new analytics-based systems to protect each channel, and link those systems as needed to provide centralized insight and control, as well as greater continuity in customer experience.

"Banks now see fraud protection as a customer service imperative, so the need to offer customers coordinated, bank-wide protection has grown," says Doug Clare, FICO's fraud chief. "However, over the past decade, the old approach to enterprise fraud management has frustrated many banks."

Clare elaborates: "Every bank will achieve enterprise fraud management differently. There is no one-size-fits-all solution. That said, the most successful fraud solutions will include a combination of predictive analytics to identify changing fraud patterns, business rules to stop known fraud types, link analysis to see broader patterns indicating fraud rings, and case management to shut down fraud with a minimum of customer interruption."

It should be mentioned that FICO, GFI Software, Guardian Analytics, and Trend Micro all offer technological solutions to fraud issues at financial institutions. It also should be mentioned that Trustwave is endorsed by ABA's Corporation for American Banking, for information security and data loss prevention.

Recently, Trustwave announced that it has teamed with Microsoft to bring an open-source web application firewall to top web server platforms.

As important as the technology is, however-whoever provides it-fraud management depends on the organization that backs it up.

Art Coviello, executive vice president of EMC and executive chairman of RSA, said as much at a global security conference held in China. He said that today "the vast majority of IT security spending is still allocated toward static and inflexible perimeter-based technologies that are increasingly ineffective against today's threats. In an age of interconnectivity and openness where breaches are to be expected even among the best-defended networks, the balance must shift to accommodate timely detection and response."

He advocates four paths the industry should follow:

- Commitment to intelligence-based security that evaluates the context of vulnerability, probability, and materiality.
- The best defense is a layered defense that delivers situational awareness, deep visibility, and environmental agility.
- The right talent must be found, meaning individuals who have applicable education, training, and experience, especially with analytic tools.
- Cooperation, in the sense of an ecosystem of governments, vendors, and user organizations that work together to foster more trust in the digital world.

Closing on a familiar note, Coviello says, "We are only as strong as our weakest link and we are interdependent as never before. Attacks on one of us have the potential to be attacks on all. We must adapt and change. The economies of the world are too fragile to run the risk of not tackling this problem head on."

Sources used in this article include:

Independent study finds that financial institutions are losing clients as a result of a single fraud attack

FICO Champions New Approach to Enterprise Fraud Management

FICO Data Shows a Spike in US Credit and Debit Card Fraud

GFI Survey Finds Majority of Small Businesses Not Confident in Network Security or Performance

RSA Chief Rallies for Intelligence-Driven Security to Help Ensure Trust in the Digital World

Companies Still Struggling with Cloud Security: Reported Higher Incidence of Data Security Lapse or Issue From 2011

Trustwave Teams with Microsoft to Bring Open-Source Web Application Firewall to Top Web Server Platforms

About the Author

John Ginovsky is contributing editor of ABA Banking Journal and editor of the publication's TechTopics e-newsletter. For more than two decades he has written about the commercial banking industry. In particular, he's specialized in the technological side of banking and how it relates to the actual business of banking. He previously was senior editor for Community Banker magazine (which merged with ABA Banking Journal) and was a staff writer for ABA's Bankers News. You can email him at jginovsky@sbpub.com