

DIEBOLD WINS SKIMMING DETECTION TECHNOLOGY AWARD



Innovative
technology reduces
ATM fraud by
sensing skimming
devices.

In this issue

[Diebold wins award for advanced
skimming detection technology](#)

[Ram raids and ATM removals
on the rise](#)

[ID theft red flags: essential elements
of customer awareness](#)

[Diebold updates consumer safety website](#)

Diebold, a trusted partner and leader in the financial self-service industry, recently announced it received The Banker Technology Awards 2008 Retail Award for Delivery Channel Security for its leading-edge ATM advanced skimming detection technology.

Diebold's advanced skimming detection technology detects the presence of skimming devices to help prevent automated teller machine (ATM) fraud and the loss of millions of dollars each year for financial institutions. This feature is included in every new Diebold Opteva(R) motorized card reader at no extra charge, which is a substantial benefit as the average industry cost for similar technology is between \$1,200 and \$1,500 per unit. The Banker Technology Awards, presented by The Banker magazine, recognize excellence and innovation in all areas of banking technology. The awards serve as a vital global benchmark for IT services, products and projects in the financial services industry at large.



Diebold is honored to receive such a prestigious award and to be recognized by the industry as a leader in ATM security, said Charles E. Ducey, Jr., senior vice president, global development and services, Diebold. The advanced skimming detection technology is designed to put our customers' minds at ease and provide reassurance that both the financial institution and its customers are protected.

ATM fraud occurs on a global scale and is a growing concern. According to estimates by Retail Banking Research, there are currently more than 1.5 million ATMs worldwide with new installations occurring every five minutes. The Global ATM Security Alliance reports that .0016 percent of all worldwide ATM transactions are affected by crime or fraud and it has been proven that skimming can account for as high as 99 percent of ATM attacks in many geographic areas. With Diebold's advanced

skimming detection solution, Diebold customers can fight growing criminal activity and reduce financial loss.

In addition to the industry's growing fraud concern, the number one concern among financial institution customers is the theft of personal financial information -- surpassing terrorism, job security and natural disasters, Ducey said.

Diebold has a rich history of delivering security solutions for more than 149 years and our customers depend on us to continue to deliver advanced technologies to secure their assets. This award truly speaks to the high-quality processes and procedures Diebold has in place as a security leader in the financial self-service industry.

To find out how you can minimize your losses due to this growing industry problem please visit Diebold ATM Security at <http://www.diebold.com/atmsecurity/security>.

The number one concern among financial institution customers is the theft of personal financial information -- surpassing terrorism, job security and natural disasters.

RAM RAIDS AND ATM REMOVALS ON THE RISE

Ram raids and physical attacks on ATMs are on the rise in many regions of the United States and other parts of the world. European ATM Security Team (EAST) reports that physical attacks on ATMs in the U.K. have increased by 65 percent.

The report says that even though the cash losses for such attacks are lower than fraud levels, the risks to people and the collateral damage to property remain a great concern to the industry. Ram raids are becoming the one of the more popular methods of attack.

The modus operandi involves thieves stealing a large construction vehicle along with another truck to ram the ATM and then load it onto the truck. This type of crime is usually perpetrated by a group of individuals who move through a locality until they have exhausted all opportunities and then move on to the

next county, state or town. These attacks can also occur with ATMs not located in banks, such as those located in convenience stores or other retail locations where they wrap a chain around the ATM and drag it out of the store. Losses associated with this type of crime can include the ATM, the cash inside and the property damaged as a result of the attack. The loss alone of the channel creates an inconvenience for your customers also which can also impact their loyalty.

The impact of these types of attacks can be mitigated by implementing a combination of security measures that help to minimize these violent attacks on ATMs.

To learn best practices for remote or offsite ATM installations click here to view the Island ATM Security White Paper.

ID THEFT RED FLAGS

Linda McGlasson, Managing Editor
BankInfoSecurity
September 2, 2008

Essential Elements of Customer Awareness

As financial institutions scramble to meet the Nov. 1 deadline for Identity Theft Red Flags Rule compliance, the operative word is "prevention" - as in Identity Theft Prevention Program.

And the key to making prevention work, observers say, is a sound customer awareness program that goes beyond statement stuffers and television ads.

Regulators have raised the bar on identity theft prevention, says Sai Huda, CEO of Compliance Coach, an industry risk management and compliance services company. "The ID Theft Red Flags Rule has created an affirmative obligation on financial institutions and creditors to take proactive steps to prevent identity theft," he says.

Regulators expect to see evidence that institutions took their obligations seriously and methodically performed an inventory of all accounts; a risk assessment to determine covered accounts; considered the 26 red flags in Appendix J to the Rule; its own historical experience and other credible sources; mapped red flags to appropriate detection and response procedures; and developed a risk-based, written Identity Theft Prevention Program.

Also, Huda says, regulators will ask 'Did the institution obtain board approval and provide appropriate employee training to effectively implement the program?' Additionally, is the financial institution periodically updating the program to address new risks or operational changes, and is it overseeing vendor and business partners to mitigate identity theft?

While there is no legal requirement to provide a notice to or educate consumers in the rules, "such proactive efforts will reflect positively on the financial institution that undertakes a consumer awareness effort and to invite the consumer to join the fight to deter identity theft," Huda says.

Elements of Awareness

Tell Them What You're Doing -- Speaking with several industry thought leaders, they all concur that awareness begins with telling customers what you're doing to protect their information. Not doing this creates the "enemy within," says Tom Wills, Senior Analyst of Risk, Security, Fraud and Compliance at Javelin Strategy and Research. "For customer-facing security awareness and education, the enemy comes from within,

as institutions are sometimes reluctant to talk about security for fear of giving too much knowledge to the bad guys." The good news is, "It's not necessary to give away your methods in order to communicate to customers and to the public about security," he adds.

Explain the Real Risks -- What institutions will want to tell their customers is that more than 8.3 million consumers fall victim to identity theft each year, and over \$15.6 billion in losses are caused by fraudsters, according to the Federal Trade Commission. Fifty percent of the time it is a business that provides the point of vulnerability to thieves to steal consumer information due to poor controls, procedures or employee training, according to the U.S. Secret Service. Identity theft is a growing crime and consumers are very concerned. "Added to that, due to the current economic conditions, banks are suffering financial losses and some are even failing," says Huda. "Consumers are becoming concerned not only about the safety of their money, but also their personal information and beginning to question the trustworthiness of their financial institution that has both their money and information."

Offer Reassurance -- Financial institutions should be proactive and clearly communicate to consumers a simple message: It recognizes that these days the consumer may have concerns about the safety of their money and personal information, and that the financial institution has taken appropriate steps to protect both their money and personal information to maintain the consumers trust. This message will reassure existing customers, but also serve as a competitive differentiator and attract new business.

Additional Points

The following are some key points that a financial institution should cover in an Identity Theft awareness program for consumers:

Identity theft harms both the consumer as well as the financial institution. It is a joint fight;

The financial institution cares deeply about the consumer's financial well-being and has taken steps to protect both their money as well as personal information;

Just as the financial institution has taken steps to do its part to fight identity theft, customers should also do their part by being alert at all time and not allow points of vulnerability for thieves;

The financial institution should list common methods of how thieves steal information and certain steps consumers should take to deter identity theft;

The customer should contact the financial institution if at any time their identity is stolen, and also a non-profit resource such as the Identity Theft Resource Center (ITRC) or the Identity Theft Assistance Center (ITAC) for counseling and assistance.

Crunch Time Before Nov. 1

With fewer than 60 days to go before institutions must comply with the new regulation, there are things that an institution can do to promote more customer awareness. One problem that Dr. Markus Jakobsson, Senior Research Scientist at the Palo Alto Research Center, sees with many customer awareness programs (not just those honing in on identity theft) is that they don't explain the problem.

"Most security education by financial institutions shows examples only -- they do not teach the underlying principles," he says. "That is like teaching kids how to recognize the 100 most common words -- but not teach them how to read!" Jakobsson, a noted information security researcher, points to the hardest hurdle - motivating customers. "Most security education fails to motivate the recipients. It is hard or boring, and as a result, only people who already have problems (and want to avoid getting phished again) bother to use the material."

Material needs to be easily accessible, and in bite-sized portions. "People buy security textbooks if they want to become security experts," Jakobsson says. "Very few people are going to buy a fat textbook about security in order to be more secure online."

Wills encourages institutions to engage their marketing and PR talent, "to treat security awareness like a marketing campaign. If done well, this can be a great brand builder for your institution because trust (which follows largely from sound security) is a key value element that customers look for in their financial institution."

KEEPING CONSUMERS SAFE

Diebold helped pioneer 24-hour access to financial accounts through the introduction of the automated teller machine. Decades later, Diebold is helping financial institutions provide consumers with unlimited access to valuable information about how they can increase their personal security at the ATM.

Diebold has recently revamped its exclusive Web site dedicated to ATM consumer safety. By linking to this site from their own site, financial institutions can provide tips to protect against crimes ranging from robbery to electronic fraud. The Web site also highlights industry news and alerts about emerging ATM crimes.

Diebold was the first ATM manufacturer to produce a Web site focused solely on ATM crime prevention. Diebold encourages financial institutions to link to the site from their own Web sites, providing their customers and members with the information they need to increase their own personal safety and better secure their personal finances. To access Diebold's consumer safety site, visit www.diebold.com/playingitsafe.

Call on Diebold for the latest in product, service and security solutions.
Since 1859, Diebold has put the customer first.

Contact Information:
Diebold, Incorporated
5995 Mayfair Road
North Canton, Ohio
44720-8077

E-mail: fraud@diebold.com
www.dieboldatmsecurity.com

Security Matters is distributed quarterly to customers of Diebold and to Diebold sales and service associates around the globe to facilitate open communication and awareness of fraud and security related issues affecting customers. If you would like to share fraud or security related issues with Diebold, please email items of interest to fraud@diebold.com.

