

PREVENTING IDENTITY FRAUD IN THE BRANCH

Preventing Identity Fraud in the Branch

Brad Stephenson, vice president of physical security, Diebold Global Security

Nearly 9 million adult Americans were victims of identity theft in 2006.¹ That translates to more than \$56 billion in financial losses,² and anywhere between 300 million to 900 million hours (depending on your source) spent by victims trying to resolve associated problems.³ Add regulatory pressures and eroding consumer confidence to the mix and it is easy to understand why U.S. financial institutions are scrambling to re-evaluate and, in most cases, redesign their approaches to protecting their customers' and members' account information.

In this paper, we will explore the root causes and effects of identity fraud and offer some new thinking and best practice solutions within the branch environment.

The Goal: Consumer Trust

The payoff for financial institutions that invest in sound security planning and systems comes not just in the form of financial risk mitigation. Reassuring security messages backed by a strong security record go a long way in building the customer trust and brand loyalty that form the bedrock of a sound financial services company. We know that more than half of Internet banking users (57 percent) would leave their bank in the event of a single security breach.⁴ And despite their online security concerns, nearly 60 percent of consumer respondents are

still more confident in online banking than in branch banking. It takes only one privacy breach to destroy a relationship, even among banks with the highest levels of consumer trust. And as consumer trust continues to be tested with mergers and acquisitions, new technology, inadequate service and other tension points, financial institutions can't afford the repercussions of online or off-line fraudsters stealing customer identities, not to mention non-customers using stolen identities for in-branch transactions.

While the financial services industry fares better than many others when it comes to consumer trust, many industry experts are citing significant slippage. Not surprisingly, we're seeing a renewed focus on one-on-one relationships, whether it's a commercial account manager dealing with a commercial client, a wealth advisor dealing with an investor or a branch manager dealing with branch customers. At the end of the day, a financial institution's success is still largely tied to the front-line employees' relationships with customers.

Focusing in on the Branch

In an industry so heavily dependent on trust and relationship building, the branch is still king. During 2004, it is

estimated that about five branches were opened per business day and about \$6 billion was spent to establish new branches.⁵ Industry research also suggests that half of American consumers say the branch is their preferred mode of interaction with their financial institution. Further, according to Accenture, a global research and technology consulting company, 42 percent of consumers visit their branch at least once per week and 86 percent are in the branch at least once per month.⁶

With so much of our daily activity being conducted in cyberspace, many consumers crave the face-to-face experience – which is good news for the banker with a good security message and appropriately trained staff to deliver that message. The trained teller can ease customers' minds by educating them about the speed, accuracy, noninvasiveness and importance of additional security measures. In some cases, the technologies themselves will do the educating, leaving tellers more time to manage and grow relationships. If the branch is going to be an important part of a bank's growth strategy, frontline associates must be able to answer questions confidently and reassure customers that their assets are secure. Aggressively communicating your security policies in the branch has other benefits, as well; namely, attracting new customers and deterring criminals.

Identity theft will continue to make headlines and threaten hard-earned consumer confidence – and, ultimately, brand equity and shareholder value – if financial institutions don't address the problem thoroughly and communicate solutions appropriately. Experience tells us that consumer perception is that banks are at least partially responsible for identity theft and should share in the responsibility. Consumers do have expectations that their financial institutions will provide identity fraud/theft prevention and detection services.

How Identity Theft Occurs

What's interesting to note is that the modus operandi of the physical security criminal has not changed since the days of Jesse James. Nineteenth century outlaws committed robbery, burglary or fraud much like the logical criminal does today – only today's criminals are accomplishing their tasks faster, easier and in dramatically higher volume.

Over the past 20 years, physical security attacks against banks have remained fairly constant but IT security attacks have increased from virtually nonexistent to nearly constant during the same period. A byproduct of advances in banking technology appears to be the revolutionizing of fraud. In addition to stealing a wallet, a credit report or mail in more traditional ways, the high-tech criminal now can steal information as it's transferred by wire or wireless technology from one place to another.

He also can "phish," that is, lure customers into providing personal financial information via phony e-mails and Web sites. According to an Anti-Phishing Working Group's July 2004 trends report, phishing attacks were growing about 50 percent each month and the financial services sector was the most targeted industry for such attacks. With a price tag to banks and credit card issuers in excess of \$1.2 billion annually,⁷ it's understandable why phishing and other similar forms of identity theft are center stage. And don't make the mistake of assuming this type of fraud is limited to online banking; criminals are walking right into the branch with stolen customer data.

The Evolution of Security

In the past, the worlds of physical security and logical security spun on completely different axes. Organizations addressed their security needs in three distinct ways:

- Physical security, such as vaults, safes, cameras, access control and alarms

- Logical security, such as the protection of sensitive information and the infrastructure on which it resides
- Security management, such as policies, procedures, regulations and security manpower

But now, astute institutions are looking at their security systems and processes holistically, addressing digital and physical security in an integrated fashion. They know that the best way to protect against white-collar crime and terrorism is to look at physical and logical security under the same lens at the same time. Likewise, as security strategies are developed, it is critical for financial institutions to consider both online and in-branch transactions, in-transit (network) and at-rest (stored) data, and long- and short-term approaches, simultaneously.

Not an easy task.

Staying current when it comes to pending regulations and changing technologies can be time-consuming and confusing. Provisions within federal legislation such as Sarbanes-Oxley, FACTA, Gramm-Leach-Bliley and the U.S. Patriot Act – not to mention regulations at the state level – have exponentially increased the number of obligations on financial institutions to protect account holders' identities and financial information.

The Federal Identity Theft Task Force created in May of this year includes 17 federal agencies and departments, which last month issued seven interim recommendations.⁸ The current Homeland Security Presidential Directive 12, which requires a uniform identification credential for employees and contractors associated with nearly 200 federal agencies, could have an impact on financial institutions in the future.⁹ The long-term intent is to require such a credential from those who interact with large corporations or financial institutions.

Best Practice Approaches

Overarching best practices we've seen that have been successful in preventing financial institution theft and fraud include:

- Implementing an enterprise level fraud reduction program (e.g., strengthening authentication requirements in the branch, as well as for other channels)
- Implementing an information protection/data privacy policy and program (e.g., network security/firewalls, identity management systems, encryption schemes, effective storage systems, remote video monitoring)
- Planning to prevent IT attacks (from both internal and external sources) in a very proactive manner, as opposed to planning to react if/when they occur
- Enhancing the bank's procurement and vendor management program, carefully selecting the right partners, then managing their interaction with your enterprise security systems and processes
- Implementing a regulatory compliance program

On the subject of regulatory compliance, guidelines issued last October by the Federal Financial Institutions Examination Council (FFIEC) call for banks to incorporate two-factor identification into their processes by the end of 2006.¹⁰ In this context, 'two-factor' means there is a second identification item used to positively and uniquely identify an individual. While this FFIEC document (Authentication in an Internet Banking Environment) addresses online banking only, the implication is that risk mitigation strategies will need to be beefed up throughout the organization. Financial institutions that are truly committed to protecting customer and member privacy are not only starting to use secondary security methods online, but they are also bringing them into the retail

environment – a move that will undoubtedly pay off.

Options for two-factor authentication in the branch include:

- A shared secret, such as a mother’s maiden name, which is easy and inexpensive to implement (level of security – low)
- Single-use passwords, which also are easy to use and inexpensive (level of security – low)
- Out-of-band authentication, which involves contacting the customer by phone or e-mail, which can be expensive for the bank and an inconvenience for the customer (level of security – moderate)
- Various hardware options, such as tokens, smart cards or biometrics, which are initially more expensive and more difficult to implement on a large scale (level of security – high)

Getting at the Solution

Regardless of your security goals or where you are in the process, start by asking yourself a few questions:

- Do you stand to lose customers to a competitor who does a better job articulating the benefits of its identity fraud prevention measures?
- Are you prepared to stop a large-scale attack across multiple channels? It takes a robust and adaptive fraud-monitoring program to do so effectively. Catching fraudsters in the act is imperative.
- Can your brand sustain even the perception that your security is not where it needs to be? Brands take years to build and trust is a primary component. Few can recover from lack of customer confidence.

It might be useful to think about your approach in three simple steps:

1. Detect incidences or threats of fraud
2. Deter would-be thieves

3. Deploy the appropriate technology and a layered security strategy

Of course, for the “3-D” approach to be successful, it’s important to incorporate the right people and processes into the mix, too.

Most financial institutions are beginning to recognize that convergence – the bringing together of the physical, logical and management components of security in a single, seamless solution – is the answer. Protecting your institution and your customers’ assets requires more than increased surveillance. It requires a holistic, cross-channel approach to risk management. Too often when activities are viewed in a vacuum, important connections are missed. When looked at in aggregate, a whole new picture can emerge.

It’s important to note that no one technology is inherently better than another; it depends on the appropriateness for the environment and the intended use. Also, some products have interoperability, contributing to successful convergence and the achievement of a layered security approach. But finding and employing the right systems and the right partner to assist in the integration can be a challenge. To help you in that endeavor, we’ve provided a list of suggested steps to selecting an integrated solutions provider. We hope you find it useful. We also encourage you to call Diebold Global Security at 1-800-642-6827 or visit our Web site at www.dieboldsecurity.com for more information.

About Diebold

Diebold Global Security is a leading security integrator with representation in every region of the world. Focusing on the sale, installation and service of security components, Diebold serves the commercial, financial, government and retail markets. Diebold Global

Security provides comprehensive protection and detection solutions that include security and facility products, government solutions, remote monitoring and retail solutions.

8. Don't be bashful. Ask the integrator for training records, permission to interview sales and management representatives and technicians, whether the integrator has full-service offices around the country, etc.

Selecting a Security Systems Integrator

Diebold offers the following practical tips for selecting a security systems integrator appropriate for your financial institution.

1. Define the scope of work. It is important to understand your organization's past, current and future security needs.
2. Internal and external – assess vulnerabilities and apply risk analysis to security operations. Know which business interruptions are acceptable and which are not.
3. Make business continuity a priority. Have a plan in place to preserve business operations in the event of a catastrophe.
4. Develop an integrated security plan. Identify security issues to be solved, who will implement the plan and who will be responsible for the system.
5. Develop a list of qualities needed in a security systems integrator. Include the number of years in business, financial health, organizational structure, core competencies, installation and service delivery capabilities, and level of integration expertise.
6. Assemble customer contact information and arrange client visits if possible. In other words, get as much relevant third-party input as possible.
7. Do your due-diligence. Know what system platforms candidates install and service, the number of trained technical staff members, whether employees are certified, how many other clients have a system similar to the one you'll have installed, etc.

- 1 Better Business Bureau, Javelin Strategy and Research, 2006 Identity Fraud Survey Report, January 2006.
- 2 The Federal Trade Commission on Identity Theft: Prevention and Victim Assistance (Langhorne, PA, December 15, 2003).
- 3 "Identity Theft: The Aftermath 2003," The Identity Theft Resource Center, September 23, 2003 <<http://www.idtheftcenter.org/idaftermath.pdf>>
- 4 Larry Ponemon, Ponemon Institute, "Security in Online Banking is Key to Customer Loyalty," June 4, 2005 <<http://www.finextra.com/fullstory.asp?id=13465>>
- 5 "Branch Boom: Folly or Forethought?" Report published by Celent, August 8, 2005 <http://www.celent.com/PressReleases/20050808/BranchBoom.htm>>
- 6 "Achieving High Performance through Improved Security Systems," Accenture, April 6, 2005 <http://www.accenture.com/Global/Research_and_Insights/By_Industry/Financial_Service...>
- 7 "Phishing: A Growing Threat to Financial Institutions and E-Commerce" by Insights (Federal Reserve Bank of Philadelphia), Fourth Quarter 2004 <http://www.phil.frb.org/src/srcinsights/srcinsights/q4si7_04.html>
- 8 "The President's Identity Theft Task Force" by Federal Trade Commission: Your National Resource About ID Theft, May 10, 2006 <<http://www.consumer.gov/idtheft/taskforce.htm>>
- 9 "Homeland Security Presidential Directive/Hspd-12" by The White House, August 24, 2004 <<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>>
- 10 "Recent industry news about identity theft" as compiled from Diebold's internal business intelligence Web site, September 6, 2006 and "FFIEC tells banks to make transactions more secure with two-factor authentication" by CR80News, November 28, 2005 <<http://www.cr80news.com/library/2005/11/28/ffiec-tells-banks-to-make-transactions-mor...>>

Contact Information:

Diebold, Incorporated
 P.O. Box 3077
 Dept. 9-B-16
 North Canton, Ohio
 44720-8077

1.800.999.3600 USA
 330.490.4000 International
 e-mail: productinfo@diebold.com
www.diebold.com



We won't rest.

© Diebold, Incorporated 2006
 All rights reserved.
 Litho in USA 11.06 File no. 97-260