

Securing Online Identities



Next-Generation Considerations for Authentication Technology and Client Protection

Executive Summary

The year-end deadline for FFIEC guideline compliance forced many financial institutions to rapidly consider and implement solutions that were designed mainly to satisfy regulators. According to an article in the October issue of *Digital Transactions*, industry experts were predicting that, as of early September 2006, 30 – 50% of institutions “had not made significant progress toward meeting the goals set out a year ago this month by the Federal Financial Institutions Examination Council.” It goes on to explain that most industry experts agree that small community banks and credit unions were the farthest behind schedule, especially in comparison to the top 100 banks.

Although the rush to meet a deadline is over, the battle to outsmart online fraudsters is not. The question remains as to what authentication technologies were wisely selected and will have the most staying-power by outsmarting the next-generation of increasingly tech-savvy fraudsters. Getting too comfortable with any online security solution could be the fatal flaw for a financial institution, in light of the dynamic nature of security concerns and the potential costs of a high-visibility security breach.

This paper summarizes the critical issues related to online security today:

- FFIEC Guidance: The Confusion and Response
- Fraud Trends: Where Are Phishers Going Now and In The Future?
- Authentication Solutions: Are They Strong or Vulnerable?
- Authentication’s Future: Next-Generation Considerations
- The Right Mindset: What More Can Financial Institutions Do to Enhance Online Security?

FFIEC Guidance: The Confusion and Response

The 2005 FFIEC Guidance required banks to perform an IT risk assessment and implement a plan to solve any identified risks. However, it did not require implementation of multi-factor authentication or any technology in particular. The non-specific nature of the initial guideline left a great deal to interpretation and may have caused some of the delays in reacting that were seen at many financial institutions.

In August 2006, the FFIEC issued an FAQ document to clarify regulator's expectations. However, the FAQ created additional confusion as financial institutions scrambled for solutions, realizing they would need to add greater security to "any transaction that involved movement of funds" and "any transaction that involved giving out personal non-public information about a customer." Many institutions initially believed enhanced security measures would only be required on those transactions they deemed high-risk – such as "wire transfers, bill payments or accounts transfers for large sums of money or when the system detected that the customer was performing a transaction from a risky region outside the U.S."

Financial institutions with systems that evaluate a transaction's level of risk and then apply additional layers of security on "high risk" transactions most likely met the bar, if they expanded their definition of "high risk." According to George Turbin, senior analyst from the Tower Group (as quoted in *Digital Transactions* magazine) "There are so many ways to approach this." He continues, "If a bank really looks at a lot of factors in assessing the risk associated with any given transaction, then it is not necessarily required that it ask challenge questions or take extra precautions on every transaction."¹

Many smaller financial institutions outsourced their risk assessment and technology recommendations to third party providers, and, although this was allowed by the FFIEC, it is yet to be evaluated how accepted or successful these types of assessments and applications were deemed overall.¹

The success of various implementations remains in question as threats of identity fraud persist and evolve.

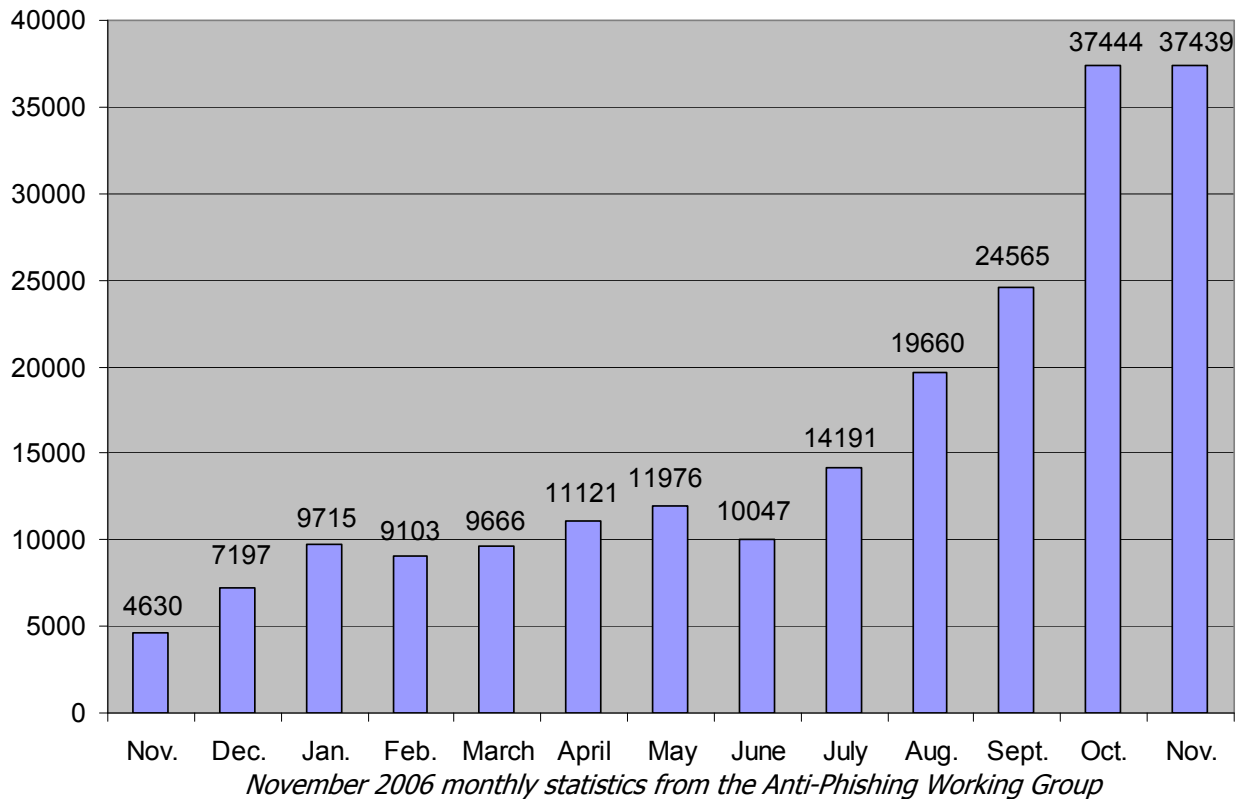
Fraud Trends: Where Phishers Are Going Now and In The Future

Are Phishers Still Attacking?

It was the slew of phishing schemes and other online fraud that prompted the FFIEC guidance requiring implementation of stronger security. And although many financial institutions were fully aware of the threats and were taking steps prior to the FFIEC guidance, it was a worthy wake-up call for others about the serious flaws that existed in their online banking and bill payment security. And now, in the wake of the year-end deadline, the threat of phishing is looming larger than ever. Are your clients safe now?

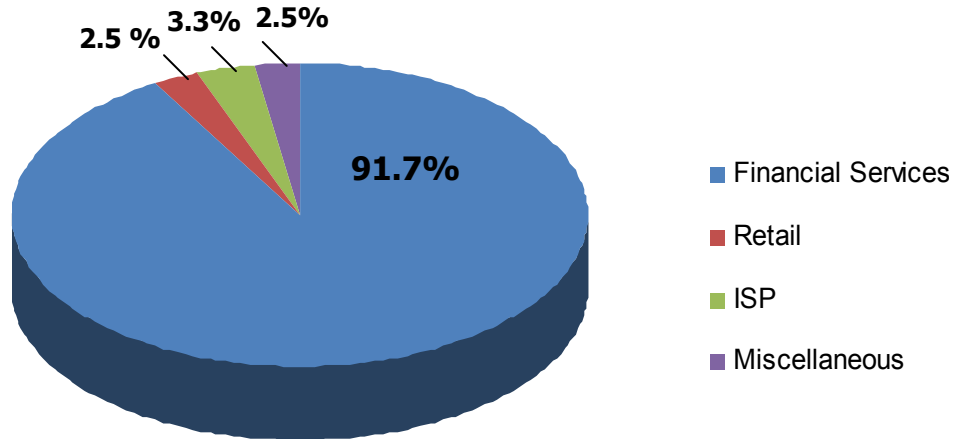
- Keylogging software schemes have increased 250 percent between January 2004 and May 2006.²
- The number of phishing alerts recorded by the Anti-Phishing Working Group multiplied a hundred-fold during this same timeframe.²
- The number of unique phishing sites has shown a general upward trend from the period between November 2005 and November 2006.³

Unique Phishing Sites by Month, Nov. 2005 – Nov. 2006



- Financial Services continues to be the most targeted industry sector with close to 92% of attacks – *November 2006 monthly statistics from the Anti-Phishing Working Group (APWG).*³

Most Targeted Sectors in Nov. 2006



November 2006 monthly statistics from the Anti-Phishing Working Group

- Phishers appear to be targeting financial institutions in waves³
- Top country hosting phishing sites remains the U.S. by a large margin (24.2%), next China (15.42%) and Korea (14.88%) in Asia, and next Germany (5.27%) in Europe – *November 2006 monthly statistics from the APWG*³

One reason for this is may be that the U.S. has the largest number of broadband connections and, therefore, our computers are more susceptible to acting as hijacked hosts for fraudsters.

- Data theft, which includes phishing-related schemes, annually costs consumers and businesses \$50 million in U.S. according to FTC statistics.²
- 10 million Americans are affected by identity theft annually according to FTC statistics.²
- A Tower Group study attributed approx. \$137 million in losses to phishing and estimated the total number of attacks to be around at around 31,000 worldwide in 2004.²
- The statistics remain high for the number of individuals responding with personal information to phishing emails. McAfee's *IdentityTheft* report from 2007 concludes from reviewing numerous studies that "between 3-5% of phishing attacks are successful."²
- Attempts to fool customers into sharing their personal information is growing and these attacks primarily target online banking services. According to the latest research released by Symantec, the company's Probe Network detected 157, 477 unique phishing email campaigns during the first 6 months of 2006, an 81% increase over the 86,906 phishing attempts it tracked during the 2nd half of 2005.⁴

- Studies are indicating that consumers are becoming more wary of online banking services.²
- APWG indicates that the number of unique phishing sites doubled during the 12 months between June 2005 and June 2006, with 93% of attacks being on customers of financial services companies. Retail, ISPs and others make up a slim percentage of those under attack.⁴

Defining the Phishing Landscape

Phishing has been defined by the Anti-Phishing Working Group (APWG) as a form of “online identity theft that employs both *social engineering* and *technical subterfuge* to steal consumers’ personal identity data and financial account credentials.”³ The APWG defines *Social engineering* as any scheme that uses spoofed emails to lead consumers to false websites where hijacked brand names of banks and other organizations convince some recipients to respond. *Technical subterfuge*, the more insidious approach, plants malware on a user’s computer for the purpose of stealing their personal credentials with a keylogger or by using a redirector to a counterfeit or authentic website with phisher-controlled proxies that intercept keystrokes.

The APWG terminology and categorization for phishing schemes are often referenced in industry articles. The APWG is a respected repository for phishing reports and is helping to track the current phishing landscape. They compile valuable statistics and attempt to define the taxonomy for phishing schemes.

Where Will Phishers Go Next?

Low-tech phishing attacks will remain with us in the near future with their combination of counterfeit emails and websites, but the buzzing concern is over what appears to be an increasing number of newer attacks that are more sophisticated and less detectable by users.⁴

Following are a handful of some of the newer schemes for phishing:

- Phishing email that points to a proxy that gets its content from a central spoofed site⁵
- A Trojan that monitors bank websites worldwide and after a user logs a spoofed page a displayed without interrupting the SSL session⁵
- Man-in-the-middle attacks that gather time-sensitive login information and then use it prior to expiration time -This attack has been used successfully against OTP password tokens used for authentication.
- Man-in-the-middle phishing attacks that allow fraudsters to retrieve user login credentials in real time using a fake URL that communicates with the actual website in real time - The attack can intercept any type of credentials sent to a site after the user has logged in.
- A scheme that acts on a vulnerability in the Vector Markup Language (VML) of Microsoft’s Internet Explorer browser to embed a keystroke logging spyware program on computers⁴
- Phishing schemes that claim to bring financial institution clients in compliance with FFIEC guidelines, asking clients to provide account and PIN information to register for a “dual authentication code”⁷
- The Trojan family known as Haxadoor, A311 Death, or Backdoor-BAC is one of the most common advanced crimewares. The Trojan waits for the user to browse a website that requires authentication. The keylogger then collects the transaction data such as username and password and send the stolen data to a dedicated host log file. There are many backdoor-BAC variants. The crimeware kit was written by a Russian named Corpse, and the toolkit sells online for \$200 - \$500.²

Although not typically categorized as phishing technology, the following technologies can be misused by criminals to phish personal information from computers.

- Commercial utilities, such as those used for parental online content control, can be used to intercept keystrokes and computer activity.²
- A Hardware keylogging device is a small recording device inserted where the keyboard cable connects to the back of a computer that can be misused to collect login information.²

The latest phishing statistics and schemes should bring attention to the need for financial institutions to stay informed and constantly evaluate the capabilities of their existing fraud prevention technologies.

Authentication Today: Is it Strong or Vulnerable?

Although it may be obvious that a next-generation of more sophisticated phishing attacks is on the horizon, many financial institutions are waiting-to-see if their solutions are now fraud-proof. And legitimately, some institutions have reason to be more confident than others.

However, most of the nation's leading financial institutions are not taking a wait-and-see approach. They are actively engaged in evaluating and testing ways to improve upon the security systems they have introduced.

Authentication technology is a primary component of many online security solutions today. Following are some of the advantages and disadvantages of the various types of authentication solutions available:

Image Verifications

- PassMark / Site-Key
- Hidden Letters

Advantages

- Good anti-phishing technology
- No new software installed on users computers
- Easy to Use

Disadvantages

- Does not gather additional verification information from the User
- Users can ignore Site-Key protection

One-Time Passwords

- Tokens
- Row/Column Bingo Cards

Advantages

- One-Time Password technology is considered to provide high levels of security
- Cross-channel possibilities

Disadvantages

- No anti-phishing component
- US Mail distribution is inconvenient for user
- Distribution costs
- Ongoing management issues, e.g. lost tokens or bingo cards

User Name: Ssmith
Password: *****
Entrust: A2 C4 F3
IdentityGuard: M 2 6
Submit



Biometrics

- Fingerprint Reader
- Voice Recognition

Advantages

- Identifies Person

Disadvantages

- Cannot change if compromised
- Hardware devices must be installed and are not readily available



- Increased support complexity

Client-Based Solutions

- Computer ID Software Generators
- Verification of H/W Tokens Existence
- Smartcards



Advantages

- Identifies user and machine, considered to provide high security

Disadvantages

- Requires users to install drivers / hardware
- Ties user to a specific PC
- Support related issues
- Can be high cost

Multi-Device Solutions for Out-of-Band Requests

- Computer + Phone or PDA

Advantages

- Eliminates man in the middle

Disadvantages

- Sacrifices ease-of-use
- Phone / wireless is not always available
- Support issues
- Cost

Expert Systems

- Host Systems Determine Deviations and Determine Risk

Advantages

- No user actions required
- Can be transparent to user if no exceptions processing

Disadvantages

- Can be spoofed
- Can provide a false sense of security
- If exception detected, then the user experience can be negative

Layered Security Approach

- Provides the best of all worlds
- Most technologies can be layered

As the technology and requirements evolve, decision makers that seek to stay informed about the strengths and weaknesses of various security solutions will be in the best position to make forward-thinking choices to protect their customers' online identities.

Take another look at what holes may remain in your online security at varying levels of transaction risk. Intelligently evaluate if solutions are adequate for now. Are there more cost-effective or secure solutions available? Could areas benefit from additional layers of security? By the time fraudsters uncover solution vulnerabilities, reactions may not be quick enough.

A recent Harvard/MIT study produced eye-opening statistics regarding the security vulnerabilities of SiteKey authentication technology. To summarize, of 60 test subjects only 2 did not enter their passwords when the Sitekey image was not present. Even worse, when the image was replaced with an obvious error message, 58 people didn't notice or didn't care that the Sitekey image was missing and entered their password anyway.⁸

Authentication's Future: Next-Generation Considerations

It is widely agreed among experts that the ideal online security for financial institutions involves a layer of multi-factor authentication for customers logging into online banking and bill payment services, followed by further analysis of transaction type and application of additional security features for those transactions categorized as higher risk.¹

Authentication technologies can and should be evaluated on all of the following criteria:

- ✓ Ability to provide a high level of protection against hacking, spyware, man-in-the-middle, and classic social-engineering phishing attacks
- ✓ Ease-of-implementation
- ✓ Cost-effectiveness
- ✓ Ease-of-use
- ✓ Level of maintenance/customer support required
- ✓ Customer mobility
- ✓ Functionality to work across multiple customer communication channels (web, ATM, PDAs, cell phone, etc.)

Keystone Authentication

Keystone Authentications was designed to offer financial institutions the advantages of easy integration, scalability, remote access, low-cost, and the best balance between high security and ease-of-use.



Superior OTP Security

One-Time-Passwords (OTP) are a proven technology for strong authentication. Keystone Authentication from AP Technology is a OTP technology combined with an anti-phishing mechanism that provides a highly effective defense against man-in-the-middle attacks.

By validating both the user and the site, Keystone Authentication effectively prevents what the Anti-Phishing Working Group has categorized as today's most sophisticated phishing attacks, such as phishing-based Trojan keyloggers or redirectors (man-in-the-middle attacks). Keystone Authentications is also an effective measure against the newer types of attacks described earlier in this paper. (See Section: Fraud Trends: Where Phishers Are Going Now and In The Future)



Cost-Effective

Securing Online Identities

©2007 AP Technology. All rights reserved. AP Technology is a registered trademark and Keystone Authentication is a trademark of AP Technology. Keystone Authentication is a patent-pending technology.

Keystone provides OTP security and simplicity, without the production and delivery costs of hardware or software-based password-generating devices. Users themselves create and print, or download to their PDA, their OTP CodeSheet.

Intuitive and Easy to Use

A user creates and prints their personal *Keystone CodeSheet*. The *CodeSheet* is used to provide *Mutual Authentication* each time they access their account:

Site Validation: User verifies the position of their *Keystone Image* in the *Image Challenge* (OTP).

The Keystone Image is an anti-phishing mechanism. The randomly-generated image appears on the users CodeSheet. During registration, the user selects the position for their Keystone Image within the Image Challenge (i.e. Position 1, 2, 3, 4).

User Validation: User decodes a randomly-generated *Image Challenge* using their *Keystone CodeSheet*.

Strong Multi-Factor Security

Keystone Authentication is multi-factor technology with an open architecture that can be tailored to a bank's required level of security. That is, customer or transaction data may be used to determine the level of security.

Increased security is achieved by increasing the:

- number of images in a given login *Image Challenge*
- number of images in a given *Image-Set*
- total number of *Image-Sets* available to customers
- or any combination thereof

Keystone One-Time Passwords can range from three to five images. User CodeSheets typically contain 21 images and are randomly generated from a much larger, user-selected set of images. The Bank also determines the total number of *Keystone Image-Sets* to place in its library.

The many variables of security built into this easy-to-use solution would confound any criminal trying to resolve the nearly infinitesimal possible combinations. Only someone with the correct username and password and the user's current CodeSheet can gain access to the user's financial data.

The Right Mindset: What More Can Financial Institutions Do to Enhance Online Security?

Now that year-end deadlines for compliance with FFIEC guidelines have come and gone, the challenge remains to implement technologies that stay in front of fraudsters. Following are a few considerations to keep in mind as you steer the right course to securing the online future of your clients and your financial institution:

- The fight against fraud is not over; more work is required.
- Stay informed regarding the latest phishing trends.
- Proactively monitor for and disable known phishing sites.
- Proactively research online fraud prevention technologies and practices and be willing to adapt and apply the best security to protect your retail and business clients.
- Apply the most effective authentication technology.
- Protect online and phone communication channels with fraud detection software.
- Incorporate notifications for suspicious or important transactions.
- Establish a layered approach to security.
- Regularly assess risk in different areas of your IT infrastructure based on emerging and existing threats; remain adaptive and forward-thinking in your approach to preventing fraud in all areas.
- Important client communications should not be sent via email.
- Educate your clients on the dangers that exist and build confidence by providing general information about the security measures your financial institution is taking to prevent phishing and identity fraud vulnerabilities.
- There are many financial institutions to attack; make sure your security is good enough to send attacks elsewhere.

References

1. "Going Down to the Wire," *Digital Transactions*, article by Lauri Giesen, October 2006.
2. "Identity Theft," white paper from McAfee by Francois Paget, January 2007.
3. "Phishing Activity Trends, Report for November, 2006", from the Anti-Phishing Working Group.
4. "Phishers Target Financial Institutions," eWEEK article by Matt Hines, October 22, 2006, http://www.eweek.com/print_article2/0,1217,a=191967,00.asp
5. 'Phishing Special Report: What We Can Expect for 2007,' White Paper by RSA Security, 2006.
6. "RSA Catches Financial Phishing Kit," eWEEK article by Patrick Hoffman, January 10, 2007, http://www.eweek.com/print_article2/0,1217,a=198397,00.asp
7. "Phishing scams using FFIEC deadline to dupe financial customers," SC Magazine, article by Frank Washkuch, November 29, 2006. <http://www.scmagazine.com.au/print.aspx?CIID=69260>
8. "Study Finds Security Flaws on the Web Sites of Major Banks," by Brad Stone, New York Times, February 5, 2007, http://www.nytimes.com/2007/02/05/technology/05secure.html?_r=2&oref=slogin&oref=slogin

Other Sources:

"E-Banking," Federal Financial Institutions Examination Council, August 2003, http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/e_banking.pdf

"Authentication in an Electronic Banking Environment," Financial Institution Letters, August 24, 2001 http://www.ffiec.gov/ffiecinfobase/resources/info_sec/fdi-fil-69-2001-authentication_in_electronic_bank_environ.pdf

"Authentication in an Electronic Banking Environment," OCC Bulletin, OCC 2005-35, http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/occ-bul_2005-35.pdf

'Bank Security News,' December 2006, Vol. 4, No. 9

"Identity theft prevention and detection: Are your branch banking customers at risk?," Unisys White Paper, copyright 2005