



# Insights

FEDERAL RESERVE BANK OF PHILADELPHIA

A newsletter published by the Supervision, Regulation & Credit Department for the institutions that it supervises.

Volume 9 Issue 2

## IN THIS ISSUE

SVP Commentary ..... 1

Phishing: A Growing Threat to Financial Institutions and E-Commerce ..... 2

Understanding the Proposed Capital Treatment of Trust Preferred Securities.....4

Introducing: Training for Community Bank Directors ..... 9

Compliance Corner..... CC1

## CIRCULATE TO:

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

### SVP Commentary on... Sarbanes-Oxley: Two Years Later

Eighteen months ago in the Second Quarter 2003 issue of *SRC Insights*, I first discussed the potential impact of *The Sarbanes-Oxley Act of 2002* on financial institutions. As I noted, many of the provisions in Sarbanes-Oxley merely codify the internal controls and corporate governance requirements prescribed for financial institutions through FIRREA, FDICIA, and the Board of Governor's Regulation O, *Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks*. I believed then and believe today that most financial institutions already have the fundamentals of corporate governance entrenched in their operations and that the significant majority of financial institutions already have rigorous processes to select qualified directors, ensure that the directors can devote an

adequate commitment of time to the bank, provide continuous director training, provide solid management information, and balance the power of the CEO and directorate.



continued on page 10

# Phishing: A Growing Threat to Financial Institutions and E-Commerce

by Frederick W. Stakelbeck, Jr., Training and Development Coordinator

My earliest memories of fishing as a child in Philadelphia were of fun, laughter, and friendship. Fishing offered my friends and me the opportunity to discuss sports, young love, and our dreams for the future. Today, those fond memories of summers past and innocent childhood pursuits have been replaced by a new kind of “phishing,” one far removed from the muddy waters of my childhood recollections.

## It's Phishing Time!

Phishing, also known as “brand spoofing” or “carding,” is a term created by hackers in the mid-1990s as a play on the word “fishing.” Phishing has become the hottest, and most troubling, new scam on the internet, according to the Federal Bureau of Investigation.<sup>1</sup> The Anti-Phishing Working Group (APWG)<sup>2</sup>—whose members include financial institutions, e-commerce and Internet service providers (ISPs),

and software vendors—defines phishing as the use of spoofed e-mails and fraudulent web sites to fool a recipient into divulging personal financial data such as credit card numbers, account

**Phishing: The use of spoofed e-mails and fraudulent web sites to fool a recipient into divulging personal financial data.**

usernames and passwords, and social security numbers. Once personal account information is obtained, accounts can be depleted, new accounts opened, online purchases completed, and electronic trades made using the victim's name.

The most common method of phishing used by cyber criminals is the “dragnet method.” Like a fisherman casting a large net to catch as many fish as possible, the dragnet method is designed to elicit responses from unsuspecting e-mail recipients. Using an e-mail message as the “hook,” recipients are directed to a fraudulent web site with falsified corporate identification. To give the appearance of legitimacy, the e-mails often contain

urgently worded phrases such as the following.

*We regret to inform you that the credit card information for your account has expired. Please enter new valid credit card information within 24 hours of receiving this e-mail.*

*Your account will be closed or suspended if you do not take the required action outlined in this e-mail. Please click on the attached link to visit our site and re-enter your account information.*

Once the e-mail recipient enters personal information into the fraudulent web site, the identity thieves have all of the information necessary to perform additional fraudulent acts using the e-mail recipient's personal identifying information.<sup>3</sup> Phishing can also occur by telephone, when a bank customer is contacted by an identity thief posing as a financial institution representative, potential employer, or sales representative, in an effort to fraudulently obtain personal information.

---

<sup>1</sup> Anti-Phishing Working Group, *Proposed Solutions to Address the Threat of E-mail Spoofing Scams*, <[www.antiphishing.org/Proposed%20Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Paper.pdf](http://www.antiphishing.org/Proposed%20Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Paper.pdf)>.

<sup>2</sup> The Anti-Phishing Working Group has been organized to develop an acceptable solution to e-mail phishing scams. The group meets periodically, but is largely coordinated via e-mail communications. The group maintains a web site at <[www.antiphishing.org](http://www.antiphishing.org)>.

---

<sup>3</sup> A diagram of the attack trees for different phishing techniques appears in a McAfee Security March 2004 whitepaper, *Anti-Phishing: Best Practices for Institutions and Consumers*, <[www.networkassociates.com/us/\\_tier2/products/\\_media/mcafee/wp\\_antiphishing.pdf](http://www.networkassociates.com/us/_tier2/products/_media/mcafee/wp_antiphishing.pdf)>.

FTC Chairman Timothy J. Muris has stated, "Phishing is a two time scam. Phishers steal a company's identity and then use it to victimize consumers by stealing their credit identities."<sup>4</sup> The list of financial institutions victimized by phishing attacks in 2003 and 2004 reads like a "Who's Who," including Bank of America, Bank One, Citizens Bank, U.S. Bank, SunTrust, MBNA, Wells Fargo, and Visa, to name a few. And, the financial services sector continues to be the most targeted industry sector for phishing attacks. For example, Citibank, with its diverse product line, wide geographical reach, and emphasis on e-banking, reported 682 unique phishing attacks in the month of July 2004 alone, 34.5 percent of the total number of phishing attacks reported by the APWG that month.<sup>5</sup> It's not only financial institutions that are coming under attack from online cyber crooks. AT&T, AOL, eBay, PayPal, Microsoft, Yahoo, the FDIC, the FBI, and the IRS have all been the victims of recent phishing assaults. No one, large or small, is immune.

### Costs of Phishing

Today's phishers and hackers are no longer phishing and hacking for the resulting thrill, but for unadulterated financial gain. The resulting cost to victimized financial institutions and consumers, in both time and money, has the potential to be enormous. A typical phishing attack can cost

a financial institution between \$50 and \$60 per account compromised, or \$50,000 per attack. Furthermore, after a typical phishing attack, it takes approximately 160 hours for IT staff to disable a phishing site (once it has been identified), reset legitimate user passwords, and install software patches. In addition to tangible monetary losses, financial institutions suffer from reduced employee and IT productivity, loss of network resources, legal liability, and damage to their brand name and reputation.

From a customer perspective, phishing attacks have become a sobering reminder of the vulnerability of the Internet and e-commerce. Trust in online payment systems and the ability of financial institutions to mitigate fraud are diminished by successful phishing attacks. According to Avivah Litan, vice president and research director at Gartner, Inc., the eventual impact of phishing attacks could slow e-commerce growth in the United States by one to two percent in 2005. "The whole promise of e-commerce—lower costs, increased revenue and quicker launches of marketing campaigns—all goes out the window if consumers cannot trust e-mail communications," says Litan.<sup>6</sup>

### Stop Phishing!

Can financial institutions adequately protect themselves and their customers from phishing attacks? According to a number of independent reports,

the answer is a resounding "YES"! If this is the case, then why has phishing become an escalating problem for the financial services industry, which has historically been extremely sensitive to IT security issues? Elazar Katz, director of Active Risk Monitoring Practice for Unisys, thinks the answer lies in the design of traditional fraud systems. "Traditional fraud systems are not designed to combat the new breed of cyber criminals," Katz says. "As criminals become more sophisticated, they are coordinating their attacks of identity theft across multiple channels. The problem is that most organizations have separate systems for credit card fraud, check fraud, and so on... and they don't usually communicate with one another."<sup>7</sup> Another fault of today's fraud detection systems, according to Katz, is a lack of focus on locations and points of usage, which allows for the free transfer of stolen information across continents, a characteristic of recent phishing attacks. A study by Next Generation Security released in September 2004 found that 90 percent of financial and commercial web sites contained flaws that, if exploited, could result in successful phishing attacks. These included site configuration problems that would allow the redirection of information from a legitimate site to a fraudulent site.

So what can financial institutions do to prevent additional phishing attacks?

*continued on page 6*

---

<sup>4</sup> Bob Sullivan, "Look-alike Email Scams on the Rise," MSNBC, July 21, 2003.

<sup>5</sup> APWG, *Phishing Attack Trends Report*, July 2004, <[www.antiphishing.org/APWG\\_Phishing\\_Attack\\_Report-Jul2004.pdf](http://www.antiphishing.org/APWG_Phishing_Attack_Report-Jul2004.pdf)>.

---

<sup>6</sup> Alice Dragoon, "Fighting Phish, Fakes, and Frauds," CIO, September 7, 2004, <[www.cio.com/archive/090104/phish.html](http://www.cio.com/archive/090104/phish.html)>.

---

<sup>7</sup> Unisys, *Banks vs. Identity Thieves: Who Will Win?*, <[www.unisys.com/services/insights/articles/articles.htm?insightsID=81290](http://www.unisys.com/services/insights/articles/articles.htm?insightsID=81290)>.

# Understanding the Proposed Capital Treatment of Trust Preferred Securities

by Vincent J. Poppa, Supervising Examiner

In January 2003, the Financial Accounting Standards Board (FASB) issued Interpretation No. 46 (FIN 46), *Consolidation of Variable Interest Entities*.<sup>1</sup> FIN 46 changed the rules for consolidating “variable interest entities,” also known as “special purpose entities” (SPE), from voting majority to concentration of risk.

Almost immediately, the accounting industry and bank holding companies (BHCs) began to wrestle with the application of FIN 46 to the then-current practice of consolidating trusts issuing trust preferred securities (TPS) with the BHC. In late December 2003, FASB issued a revised version of FIN 46.<sup>2</sup> In that guidance, the accounting authorities generally concluded that such trusts must be deconsolidated in financial statements prepared under GAAP.

Since the majority of the risks inherent in a TPS-issuing trust are borne by the TPS holders rather than the BHC, FIN 46 will not allow the trust to be consolidated with the BHC. As a result, the BHC’s consolidated balance sheet will no longer reflect TPS in minority interest, but rather will reflect the subordinated debt issued to the deconsolidated trust. The subordinated debt will be reported in other

liabilities and the equity investment in the SPE will be reported in investments in unconsolidated subsidiaries on the balance sheet. This change in accounting rules raised the question of whether the Federal Reserve would change its capital guidelines with respect to TPS, because the subor-

**The Federal Reserve is not bound by GAAP accounting in its definition of tier 1 or tier 2 capital, because these are regulatory constructs designed to ensure the safety and soundness of banking organizations.**

ordinated debt shown on the balance sheet would ordinarily only qualify as tier 2 capital.

On May 6, 2004, the Federal Reserve Board issued for comment a proposed rule that would continue to allow TPS to be counted in tier 1 capital of BHCs, subject to stricter quantitative limits. There were several reasons why the Board proposed to continue the tier 1 capital treatment for TPS. First, while the accounting designation has changed, the structure and substance of the securities have not. TPS continue to offer BHCs significant equity-like features—long lives, deferral rights, and loss absorbency. They also do not affect the BHC’s liquidity position, are easier and more cost-efficient to issue and manage, and are more transparent and better understood by the market. Since their introduction in the year 2000, pools of

TPS have given small BHCs access to the capital markets for tier 1 capital. The Board is also aware that foreign banks have issued similar tax-efficient tier 1 capital instruments, so large U.S. BHCs could have a competitive disadvantage if they were unable to count TPS in tier 1 capital.

The regulatory reporting of TPS will reflect GAAP accounting requirements. However, the Federal Reserve is not bound by GAAP accounting in its definition of tier 1 or tier 2 capital, because these are regulatory constructs designed to ensure the safety and soundness of banking organizations.

The proposed rule would apply the 25 percent of tier 1 capital limit after deducting goodwill. Previously the limit was 25 percent of tier 1 capital before deducting goodwill. Deducting goodwill from core capital elements will help ensure that a BHC is not unduly leveraging its tangible equity. This will mean that many BHCs carrying goodwill on their balance sheets may count less of their TPS in tier 1 capital.

Also, capital elements to be included

<sup>1</sup> FASB Interpretation No. 46 is available on FASB’s web site at <[www.fasb.org/pdf/fin%2046.pdf](http://www.fasb.org/pdf/fin%2046.pdf)>.

<sup>2</sup> The December 2003 revisions to FIN No. 46 are available on FASB’s web site at <[www.fasb.org/pdf/fin%2046R.pdf](http://www.fasb.org/pdf/fin%2046R.pdf)>.

in determining the limit would include minority interest that is not in the form of common or noncumulative preferred stock issued directly by a subsidiary bank or thrift. An example of the type of minority interest to be limited would be REIT preferred securities. To further guard against potential over-reliance on TPS and other non-equity elements within a BHC's capital structure, amounts of TPS and minority interest in consolidated non-depository institution subsidiaries in excess of the 25 percent limit would be included in tier 2 capital, subject, together with subordinated debt and limited-life preferred stock, to a 50 percent of tier 1 limit.

The proposal also provides that in the last five years before the subordinated debt matures, TPS would be excluded from tier 1 capital and counted only as tier 2 capital, subject to the 50 percent of tier 1 limit. During those last five years, the TPS would be amortized out

of tier 2 capital by one-fifth each year and excluded totally during the last year. That is the same haircut applied to subordinated debt and limited life preferred stock.

The proposed rule notes that internationally active BHCs would "generally be expected" to adhere to a 15 percent limit, which comes from the 1998 international Basel guideline.

As proposed, the new limits would become fully effective on March 31, 2007, after a three-year transition period that would start on March 31, 2004. However, the Board of Governors did receive 36 comments on the proposal and is considering whether any amendments to the proposal appear to be warranted. After considering the comments, the Board anticipates issuing the final rule by year-end 2004 or early 2005.<sup>3</sup>

Based upon the June 30, 2004 regulatory report filings, only three institutions in the Third District could be affected by the proposed change. However, given the amount of time to comply with the stricter limits, these institutions may not be impacted at all by the end of the phase-in period.

If you have any questions concerning the proposed capital treatment or regulatory reporting of trust preferred securities, please contact Supervising Examiner Vincent J. Poppa (vince.poppa@phil.frb.org) at (215) 574-6492. ■

---

<sup>3</sup> The comments received on this and other regulatory proposals are available on the Board of Governors' web site at <[www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm](http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm)>.

## Current Fraud Management Techniques in Consumer Lending

The October 2004 issue of *The RMA Journal* included a series of articles that focused on fraud risk, management, and prevention. Michael E. Collins, senior vice president of the Supervision, Regulation and Credit department at the Federal Reserve Bank of Philadelphia authored one of those articles—"Current Fraud Management Techniques in Consumer Lending." In this article, Mr. Collins discusses fraud mitigation techniques and issues affecting consumers, credit card issuers, and merchants. He closes by discussing the relationship between fraud and enterprise-wide risk management and bank management's role in preventing fraud.

RMA members can log on to RMA's web site at <[www.rmahq.org](http://www.rmahq.org)> to obtain a free copy of the article. Non-members can research and download *The RMA Journal* articles for a fee at <[www.rmahq.org/publications/journalad.htm](http://www.rmahq.org/publications/journalad.htm)>.

# “Phishing: A Growing Threat” continued from page 3

In a March 2004 white paper, *Anti-Phishing: Best Practices for Institutions and Consumers*, Gregg Tally, Roshan Thomas, and Tom Van Vleck of McAfee Security suggested best practices for corporations and consumers.<sup>8</sup> The authors suggested the following best practices options for corporations to reduce the threat of phishing attacks.

- Establish corporate policies and communicate them to consumers.
- Provide a way for the consumer to validate that the e-mail is legitimate.
- Provide stronger authentication at web sites.
- Monitor the Internet for potential phishing web sites.
- Implement good quality anti-virus, content filtering, and anti-spam solutions at the Internet gateway.

In addition to the preventative best practices outlined above, there are additional steps financial institutions should take when victimized by a phishing attack.<sup>9</sup> First, the institution should contact the domain name

register and attempt to get the name revoked. Second, the local high tech crime unit or Electronic Crimes Task Force should be informed. Third, the Internet service provider hosting the site should be contacted to disable the site. Fourth, e-mail monitoring and filtering capabilities should be reviewed and enhanced, if warranted.

Tally, Thomas, and Van Vleck also suggested the following best practices options for consumers to reduce the threat of phishing attacks.<sup>10</sup>

- Automatically block malicious/fraudulent e-mail by using spam detectors.
- Automatically detect and delete malicious software, such as Spyware.
- Automatically block outgoing delivery of sensitive information to malicious parties using targeted software.
- Be suspicious and follow-up to verify the authenticity of an institution.

Government agencies have also issued guidance to help consumers identify and protect themselves from phish-

ing attacks. On September 24, 2004, the FTC issued a warning concerning phishing attacks and referred victims to its identity theft web site. The agency provided the following tips to avert phishing scams.<sup>11</sup>

- Do not respond to e-mails or pop-up messages that request personal or financial information.
- Do not e-mail personal or financial information, due to its insecure nature.
- Review credit and debit card statements to determine if there are any unauthorized charges.
- Use anti-virus software and keep it current.
- Be cautious of opening e-mails or downloading any files from e-mails regardless of who may have sent the e-mail.
- Report suspicious activity to the FTC's Identity Theft Web site at <[www.consumer.gov/identitytheft/](http://www.consumer.gov/identitytheft/)>.

## **Punish Phishers!**

Special Agent John Curran, Supervisory Special Agent with the FBI's

---

<sup>8</sup> Gregg Tally, Roshan Thomas, and Tom Van Vleck, *Anti-Phishing: Best Practices for Institutions and Consumers*, <[www.networkassociates.com/us/\\_tier2/products/\\_media/mcafee/wp\\_antiphishing.pdf](http://www.networkassociates.com/us/_tier2/products/_media/mcafee/wp_antiphishing.pdf)>.

---

<sup>9</sup> Melisa LaBancz-Bleasdale, *Executive Conversation: Attacking the Phishing Threat – What Every Company Needs to Know*, August 9, 2004, <[www.net-security.org/article.php?id=721](http://www.net-security.org/article.php?id=721)>.

<sup>10</sup> Gregg Tally, Roshan Thomas, and Tom Van Vleck, p. 8.

---

<sup>11</sup> FTC, *How Not to Get Hooked by a “Phishing” Scam*, <[www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm](http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm)>.

# “Phishing: A Growing Threat” continued from page 6

Internet Crime Complaint Center, commented about the elusiveness and unpredictable nature of phishing attacks, “I’ve been to meetings of industry experts where it’s taken them minutes of studying an e-mail from a phisher site to determine that it’s not the actual site. You can’t expect the average person surfing the Internet or doing online banking to be suspicious of an e-mail that convincing.”<sup>12</sup> So, while an ounce of prevention is worth a pound of cure, effective enforcement and punishment does play a role in the fight against phishing.

Because they use fraudulent statements to mislead and deceive individuals into disclosing personal data, phishers may violate a host of federal criminal statutes in the areas of identity theft, wire fraud, credit card fraud, bank fraud, computer fraud, and laws related to computer systems and files. Sentences for these federal offenses can range from 5 to 30 years, with fines as high as \$250,000.

Of course, to enforce laws, there must be laws to enforce. While existing legislation—such as the July 2004 *Identify Theft Penalty Enhancement Act*, *Identity Theft and Assumption Deterrence Act of 1998*, *Fair and Accurate Credit Transactions Act of 2003*, *USA PATRIOT Act*, and *Gramm-Leach Bliley Act*—all contain provisions related to identity theft and/or fraud,

legislation has been introduced to specifically address phishing. In July 2004, Sen. Patrick Leahy introduced S. 2636, *The Anti-Phishing Act of 2004*, to criminalize Internet scams involving fraudulently obtaining personal information.<sup>13</sup> The bill would prohibit the creation of e-mail that would induce any person to transmit, submit, or provide any means of identification to another person for the purpose of committing a crime or identity theft. Given that fraudulent web sites are usually in operation for only a short period of time (on average 54 hours); that cyber criminals are flexible and react to bank and law enforcement countermeasures; and that an increasing number of phishing attacks are originating from overseas locations, the proposed legislation, while a good first step, will no doubt need to be revisited at some point in the very near future.

Using legislation as a deterrent is necessary, but used alone it will not stop the increase in phishing attacks. The profitability of these attacks, elusiveness of the Internet, and low risk associated with being caught, continue to make phishing an attractive criminal enterprise.

## **Banking Regulatory Action**

As phishers get better at mimicking genuine e-mails and web sites and the risks to consumers grow, the bank su-

pervisory and regulatory community has also weighed in. To help banking customers better understand the dangers associated with phishing, on September 8, 2004 the federal bank, thrift, and credit union agencies released a brochure, *Internet Pirates Are Trying to Steal Your Information*.<sup>14</sup> The brochure explains the basics of phishing and steps for consumers to take if they become victims of identity theft.

On September 10, 2004, the Federal Deposit Insurance Corp. (FDIC) issued a special consumer alert (SA 66-2004) about the increasing threat posed by phishing.<sup>15</sup> Eight months after the banking regulator itself was attacked by a similar e-mail scam, which used its name to defraud bank customers, the agency has increased its efforts to stop the spread of phishing attacks upon American consumers.

In March 2004, the Office of Thrift Supervision (OTS) released a CEO Letter related to phishing. CEO Letter 193, *Phishing and E-Mail Scams*, from Scott M. Albinson, Chief Executive Officer, provides guidance on how financial instructions can prevent, mitigate, and respond to phishing schemes.<sup>16</sup>

---

<sup>12</sup> Alice Dragoon, “Fighting Phish, Fakes, and Frauds,” CIO, September 7, 2004, <[www.cio.com/archive/090104/phish.html](http://www.cio.com/archive/090104/phish.html)>.

---

<sup>13</sup> GPO. S. 2636, *The Anti-Phishing Act of 2004*, <[frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108\\_cong\\_bills&docid=f:s2636is.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s2636is.txt.pdf)>.

---

<sup>14</sup> Federal Reserve Board of Governors, *Internet Pirates Are Trying to Steal Your Information*, <[www.federalreserve.gov/consumers.htm](http://www.federalreserve.gov/consumers.htm)>.

<sup>15</sup> FDIC, *FDIC Consumer Alerts – Phishing Scam*, <[www.fdic.gov/consumers/consumer/alerts/index.html](http://www.fdic.gov/consumers/consumer/alerts/index.html)>.

<sup>16</sup> OTS, *CEO Letter 193*, <[www.ots.treas.gov/docs/2/25193.pdf](http://www.ots.treas.gov/docs/2/25193.pdf)>.

## What the Future Holds

As both a society and global community, we are in the midst of an identity theft epidemic. An estimated 57 million American consumers have received a fraudulent e-mail, with reported losses realized by banks and credit card issuers reaching \$1.2 billion in 2003. According to a recent *New York Times* article, consumers worldwide can expect to incur losses in the area of \$20 to \$30 billion for 2004, as online attacks continue.<sup>17</sup> A recent study conducted by the Ponemon Institute, a non-profit organization, revealed 76 percent of consumers are experiencing an increase in phishing incidents and at least 35 percent receive fake e-mails at least once a week.<sup>18</sup> A consensus opinion exists among Internet experts that phishing attacks will continue to rise before they fall.

The most damaging result from the rise in phishing attacks is the potential loss of trust by consumers in the elasticity and stability of e-commerce. If American consumers, searching for a balance between security and functionality, feel that this trust is jeopardized, they may be less likely to use the myriad e-commerce tools at their disposal, regardless of the associated convenience or cost savings.

But not all is doom and gloom. Positive steps have been taken in the

areas of consumer education and in the improvement of technology available to detect and defeat phishing attacks. Working with law enforcement, Internet service providers, e-mail administrators, and industry groups, positive results have occurred through innovative actions by many of the individuals and companies that made e-commerce a reality. In particular, financial institutions have gained a better understanding of the operational aspects of phishing attacks during the past year, allowing them to develop preventive measures and establish barriers to reduce the real threat of phishing.

The most important action that can be taken to reduce the threat of phishing attacks upon financial institutions is global cooperation that reaches beyond political and geographic boundaries. Education, another key ingredient in any targeted response, is not a panacea.

The Financial Services Technology Forum has offered six key findings on phishing that may be useful in future discussions.<sup>19</sup>

1. **The need for action is clear.** A sense of urgency exists among financial institutions to find a viable solution to phishing attacks, which are growing in their effectiveness and complexity.
2. **No single solution is possible, and industry coordination is essential.** An approach that combines customer awareness/

education, technology, and legislation/enforcement is paramount. Any approach must involve all interested parties. Attacks will continue to focus on the most vulnerable points in the payment system, requiring an industry-wide approach for consistency and visibility.

3. **In addressing the problem, financial institutions must seek a financial institution specific set of remedies.** There are special financial institution requirements that do not exist in other industries. For financial institutions, the customer impact is much greater, reputational risk is higher, and confidentiality is of paramount interest.
4. **Any solution set for financial services must be evaluated against nine criteria sets, each with their own financial institution specific requirements.** The nine criteria sets include customer ease of use and acceptance; effectiveness against the problem; time to market; coordination requirements; cost and complexity of implementation to all parties; legal, regulatory, and enforcement requirements; standards based; openness; and interoperability.
5. **Our knowledge is good, but scattered, and cannot be brought to bear effectively yet.** There is a general lack of knowledge in the areas of threat models and solutions. There is still no knowledge repository in the United States regarding phishing and no reporting and information sharing capability.

---

<sup>17</sup> Financial Cryptography, *Phishing an Epidemic, Browsers Still Snoozing*, June 15, 2004, <[www.financialcryptography.com/mt/archives/000153.html](http://www.financialcryptography.com/mt/archives/000153.html)>.

<sup>18</sup> FreshNews.com, *U.S. Consumer Loss to Phishing Fraud to Reach \$500 Million*, September 29, 2004.

---

<sup>19</sup> Financial Services Technology Consortium, *Project Proposal: Counter-Phishing Initiative*, <[www.fstc.org/projects/counter-phishing-phase-1/](http://www.fstc.org/projects/counter-phishing-phase-1/)>.

6. **Coordination is critical to success and to finding timely, effective, low-cost solutions. There is currently no uniform framework in place to specify financial institution requirements, evaluate solutions, or develop options.** Financial institutions are addressing the problem of phishing individually, defining their own best practices, strategies, and investment options.

This fragmented approach may invite greater exploitation by cyber criminals and the possibility of redundancy of efforts.

We are now in an age of e-commerce where the rapid pace of growth of the Internet has inadvertently created opportunities for identity thieves to exploit certain innate systemic vulnerabilities. Fueled by robust advances in technology and an increasingly skilled

populace familiar with the nuances of online financial transactions and activities, financial institutions are faced with a daunting task. The potential impact upon American consumers and the potential for interruption of the nation's payments system cannot be dismissed. In the end, the responsibility for preserving consumer trust in e-commerce falls to us all, since we all have a stake in its survival. ■

## Introducing: Training for Community Bank Directors

In September, the Federal Reserve System announced the availability of an online training course for bank directors, *Insights for Bank Directors: A Basic Course on Evaluating Financial Performance and Portfolio Risk* ("Insights"). This course is based on an existing facilitator-led course that was developed by staff at the Federal Reserve Bank of Kansas City and used extensively in their District. System staff developed this online course to provide an alternate mechanism for delivery of the existing program when the facilitator-led session is not practical. Insights can be accessed on the Federal Reserve Bank of St. Louis's public web site at <[www.stlouisfed.org/col/director/agenda.htm](http://www.stlouisfed.org/col/director/agenda.htm)>.

Insights is an introductory course designed primarily for new outside directors of community banks who have little banking experience. However, directors at larger institutions and more seasoned directors also may find the course useful as a refresher in carrying out their responsibilities.

The course focuses primarily on gauging a bank's risk-taking and the effectiveness of its risk management.

Within this context, the course provides an introduction to corporate governance and director duties and responsibilities, covers basic bank financial analysis, and discusses portfolio risk (credit, liquidity, and market

The course takes approximately eight hours to complete. Directors may go through the course in its entirety or select individual modules most useful to them. For those that elect to review the course in its entirety, the content is subdivided into sections that take between 15 to 30 minutes to complete, allowing directors to complete the course at their own pace rather than in one continuous session.

The course includes both text and video footage. If directors choose to view the video footage, they will need a high-speed connection to the internet and Macromedia Flash player version 6.0. If their internet connection is not high-speed and they are using a dial-up connection through the telephone, they can read the video transcripts and will still be able to view all pages in the course.

To ensure that directors in the Third District have immediate access to this information, we have created a page as part of SRC's public web site that announces the availability of this program. Users can link to that page directly from SRC's home page at <[www.philadelphiafed.org/src/index.html](http://www.philadelphiafed.org/src/index.html)>. ■

### Meeting Agenda

#### How to Use this Course

- 1. Call to Order**  
*(Your Job as a Bank Director)*
- 2. Financial Report**  
*(Evaluating Financial Performance)*
- 3. Harvard Westerman Loan**  
*(A Large Loan That May Present Policy Exceptions)*
- 4. Sam Wilson Loan**  
*(Regulatory Issues in Lending)*
- 5. Allowance for Loan & Lease Losses (ALLL)**
- 6. Asset & Liability Committee**  
*(Market and Liquidity Risk)*

risk) management. It includes exercises and examples to reinforce points made in the study text. Additionally, it provides tools and links to internet sites that directors might find useful in their board oversight, making it a good reference tool.

# COVER STORY

## “Sarbanes-Oxley: Two Years Later” *continued from page 1*

However, as they say, the proof of the pudding is in the eating, and we are finding more anecdotal evidence that compliance with the intricacies of Sarbanes-Oxley is more difficult than originally anticipated. Based on comments at our recent Bankers’ Forums, section 404, in particular, is of increasing concern to many Third District institutions.

On June 17, 2004, the Securities and Exchange Commission approved the Public Company Accounting Oversight Board’s (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Conducted in Conjunction With an Audit of Financial Statements*. The 161-page Auditing Standard No. 2, which addresses audits of internal control over financial reporting required by Section 404(b) of the Sarbanes-Oxley Act, is effective for fiscal years ending on or after November 15, 2004 for accelerated filers and for fiscal years ending on or after July 15, 2005 for all other filers. The issues in this area are so complex that the PCAOB has issued three documents addressing a total of 36 questions and answers related to internal control over financial reporting.<sup>1</sup>

Due to their limited resources, many small public institutions are find-

ing it difficult and costly to keep up with the documentation of internal controls required under section 404. Some bankers have stated that as much as five percent of earnings are being allocated toward section 404 compliance. Others have noted that the costs of documenting internal control reviews, which had been documented in the past but which now must be documented consistent with the standards necessary under section 404, has tripled. Many bankers report that a large part of the increase is driven by higher audit fees. In addition, some small institutions are finding it difficult to hire external auditors to perform the internal controls audit in conjunction with financial statement audits since firms’

scarce resources are focused on their larger clients. Finally, even when an external auditor is hired, it is taking financial institutions and their auditors a significant amount of time to work through all of the section 404 requirements, and many companies believe they will not be ready by the prescribed deadlines.

Other challenges, for institutions both large and small, arise when a merger is consummated near year-end. While pre-merger due diligence activities, under most circumstances, include a review of internal controls, typically a review of the scope required by section 404 is not performed. However, some relief might be available in this area. The SEC does have a process to

### **SEC. 404. Management Assessment of Internal Controls.**

(a) **RULES REQUIRED.**—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

- (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
- (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) **INTERNAL CONTROL EVALUATION AND REPORTING.**—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

---

<sup>1</sup> The PCAOB’s *Staff Questions and Answers* documents are available on its web site at <[www.pcaobus.org/Standards/staff\\_questions\\_and\\_answers.asp](http://www.pcaobus.org/Standards/staff_questions_and_answers.asp)>.

consider management requests to limit the scope of management's assessment of internal control over financial reporting under certain circumstances, which might include when a merger is consummated near year-end and a complete assessment of the target institution's internal controls before the financial statement issuance date is not practical. When management is granted this scope waiver, PCAOB Standard No. 2 allows the auditor to limit the audit in the same manner and report without reference to the limitation in scope, subject to an evaluation of the reasonableness of management's conclusion.

### **Publicly Held Banking Organizations**

The federal banking agencies are aware of the concerns of institutions subject to both section 404 and Part 363 of the FDIC's regulations (also known as FDICIA 112). In general, publicly held banking organizations that are subject to both section 404 and Part 363 may submit a single report to satisfy both the SEC and Part 363 requirements if the report meets the following five tests.

- The report is prepared at the issuer (holding company) level.
- The report identifies the internal control framework used by management.
- The report encompasses controls for SEC financial statements and federal banking agency regulatory reports.
- The report discloses any material weaknesses.
- The report is attested to by a registered public accounting firm.

On November 17, 2004, the FDIC issued FIL-122-2004, *Annual Audit and Reporting Requirements Internal Control Attestation Standards for Independent Auditors*.<sup>2</sup> FIL-122-2004 provides additional guidance in this area, including guidance on reporting when an institution subject to Part 363 is a subsidiary of a public company but is not itself a public company.

### **Non-Publicly Held Banking Organizations**

SR Letter 02-20, *The Sarbanes-Oxley Act*, which was issued on October 29, 2002, discussed the main provisions of the Act and their potential application to publicly traded banking institutions.<sup>3</sup> SR 02-20 noted that banking organizations that are not public companies generally are not covered by the provisions of the Act, but may be subject to similar requirements under other laws or Federal Reserve or FDIC regulations. For example, insured depository institutions with total assets of \$500 million or more must have an annual audit conducted by an independent public accountant and must have an audit committee composed entirely of directors that are independent of management. Top-tier bank holding companies that are required to file a FR Y-6 and that have total assets of \$500 million or more must also have

---

<sup>2</sup> FIL-122-2004, *Annual Audit and Reporting Requirements Internal Control Attestation Standards for Independent Auditors*, is available on the FDIC's web site at <[www.fdic.gov/news/news/financial/2004/fil12204.html](http://www.fdic.gov/news/news/financial/2004/fil12204.html)>.

<sup>3</sup> SR 02-20, *The Sarbanes-Oxley Act*, is available on the Board of Governors' public web site at <[www.federalreserve.gov/boarddocs/SRLETTERS/2002/sr0220.htm](http://www.federalreserve.gov/boarddocs/SRLETTERS/2002/sr0220.htm)>

an annual audit of their consolidated financial statements conducted by an independent public accountant. These audits should be conducted following the AICPA's existing internal control attestation standards in AT-501.<sup>4</sup> These requirements should not be confused with Sarbanes-Oxley requirements, since they existed before the legislation passed in 2002 and, in fact, were considered by Congress when Sarbanes-Oxley was written.

Additional guidance for nonpublic banking organizations is available in the FDIC's FIL-122-2004.

### **The Future**

As the Federal Reserve System and other banking regulators work through section 404, PCAOB Standard No. 2, and other accounting and disclosure issues, the number and pace of which have accelerated in the wake of corporate scandals, we will continue to ensure that safety and soundness principles remain part of the dialogue. This has already taken place in areas such as the interrelationships between Sarbanes-Oxley and Regulation O; loan loss provisions and allowances; loan participations; and impairment. Dialogue between the bank supervisory agencies and the FASB, AICPA, and SEC remains an important contributor to sound public policy.

Regulations and policies that are misaligned with market realities will, in all likelihood, not be sustained, and we should expect to see further

---

<sup>4</sup> AT 501 and other authoritative standards for auditors of nonissuers are available on the AICPA's web site at <[www.aicpa.org/members/div/auditstd/auth\\_lit\\_for\\_nonissuers.htm](http://www.aicpa.org/members/div/auditstd/auth_lit_for_nonissuers.htm)>.



FEDERAL RESERVE BANK  
OF PHILADELPHIA

**The views expressed in this newsletter are those of the authors and are not necessarily those of this Reserve Bank or the Federal Reserve System.**

Editor.....Cynthia L. Course

*SRC Insights* is published quarterly and is distributed to institutions supervised by the Federal Reserve Bank of Philadelphia. The current and prior issues of *SRC Insights* are available at the Federal Reserve Bank of Philadelphia's web site at [www.philadelphiafed.org](http://www.philadelphiafed.org). Suggestions, comments, and requests for back issues are welcome in writing, by telephone (215-574-3760), or by e-mail ([cynthia.course@phil.frb.org](mailto:cynthia.course@phil.frb.org)). Please address all correspondence to: Cynthia L. Course, Federal Reserve Bank of Philadelphia, SRC - 7th Floor, Ten Independence Mall, Philadelphia, PA 19106-1574.

refinement and practical application of many of today's rules. Nevertheless, the current environment and the need to restore confidence in financial markets have taken us to where we are today. Ethical behavior, sound execution, and prudent business practices will help us set a new regulatory steady state.

Finally, while you work to ensure compliance with section 404 and other regulations, it is important not to lose sight of the need to think strategically and continue to make sound business decisions. ■

## E-Mail Notification Service

Would you like to read *SRC Insights* and *Compliance Corner* on our web site up to three weeks before they are mailed? Sign up for our e-mail notification service today at [www.philadelphiafed.org/phil\\_mailing\\_list/dsp\\_user\\_login.cfm](http://www.philadelphiafed.org/phil_mailing_list/dsp_user_login.cfm).