

SRC Insights

FEDERAL RESERVE BANK OF PHILADELPHIA



SVP Commentary on...

A Look Back at 2005 and Expectations for 2006

by Mike Collins, Senior Vice President

In the first quarter 2005 issue of *SRC Insights*, I discussed several issues I believed were worthy of close management attention during 2005. These included accounting, auditing, and internal controls; compliance risk, credit risk, and interest rate risk; and mergers and acquisitions. As we enter another new year, I think it is prudent to revisit these topics, since some still require close attention, and also to look ahead to examine how these and other issues, including information security, ethics, business continuity, competition for talent, and Basel, could impact banking organizations in 2006. Banking organizations continue to face challenges; however, they have proven themselves to be resourceful when faced with such demands.

Accounting, Auditing, and Internal Controls

Broadly speaking, financial reporting is still about measuring performance, disclosing information, and creating the infrastructure to ensure confidence and integrity in financial statements. Accounting, auditing, and internal control issues continue to provide challenges for management. In 2005, accelerated filers completed the first cycle of Sarbanes-Oxley Section 404 reporting (SOX 404)—management’s report on internal control over financial reporting and the related auditor’s report on management’s assessment—and the majority of comments received by regulators on this new reporting

requirement were negative. While the industry recognized that certain benefits were achieved from implementing SOX 404, the overall consensus was that the increased costs outweighed the recognized benefits. In response, regulators released additional guidance in May

continued on page 6



2

Spyware: A Hidden Danger for Financial Institutions

4

Authentication in an Internet Banking Environment

9

Check out FR Y-10 Online!

9

Introducing the New FR Y-10S Regulatory Report

CC1

Compliance Corner

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 on the Federal Reserve Bank of Philadelphia's website at 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). Please address all correspondence to: Cynthia L. Course, Federal Reserve Bank of Philadelphia, SRC - 7th Floor, Ten Independence Mall, Philadelphia, PA 19106-1574.

EditorCynthia L. Course
Associate Editor.....Joanne Branigan
Designer.....Dianne Hallowell

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.



Spyware: A Hidden Danger for Financial Institutions

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

A growing number of American corporations and consumers use the Internet for online banking services. Destructive electronic threats to consumer and institutional privacy, combined with an unprepared or inadequate security infrastructure, have turned “e-commerce” into “e-caution.” One of the main reasons for the growing sense of angst among consumers and corporations is spyware.

Spyware monitors user activity on the Internet and transmits the information collected to an undisclosed and unauthorized third party. It is often bundled with free software that disguises its true intentions, most commonly in the form of adware, a series of pop-up advertisements.¹ Some spyware and adware track keystrokes to capture passwords and logins, social security numbers, credit card numbers, and bank account information. The intentional theft of one or more of these proprietary identifiers poses a profound security risk for any organization, especially a financial institution.

Spyware can be installed on a user's computer in several ways, including:

- Downloading a bundled shareware or other software program, such as a music CD containing a Trojan horse.² The Trojan horse surreptitiously smuggles a damaging spyware program into the user's computer.
- Falling victim to a phishing scam, which uses misleading e-mails to collect personal information.
- Viewing a pop-up that later installs spyware programs without the user's knowledge.
- Downloading free preventive spyware software, when spyware is actually installed.

Signs of spyware on a user's computer include sluggishness, pop-up inundation, hijacked home pages, or redirection to unintended sites. Spyware can resemble a computer virus, but they have some impor-

¹ Adware is a type of advertising display software whose primary purpose is to deliver advertising content in a manner or context that may be unexplained to and unwanted by users (Anti-Spyware Coalition, *Definitions and Supporting Documents*, July 2005).

² A Trojan horse is a nonreplicating malicious program designed to appear harmless or even useful to the user, but, when executed, harms the user's system (Anti-Spyware Coalition, *Definitions and Supporting Documents*, July 2005).

tant differences. A virus is a self-replicating program that seeks to infect a computer and spreads by embedding itself into a program code or document, taking advantage of poor user security habits to infect as many computers as possible in a rapid manner.³ While viruses seek to spread unabated, spyware is more stationary. It does not replicate; instead, it takes partial control of a computer's operation without the user's knowledge by persuading the user to download and install the malicious program in order to collect personal data.

The inaugural *State of Spyware Report* released in May 2005 by Webroot Software, a manufacturer of anti-spyware software, shows a troubling trend of spyware infiltration.⁴ Webroot's analysis showed that 92 percent of all computers were infected with spyware in the last quarter of 2004 and 88 percent in the first quarter of 2005. The report also claims that spyware products generate \$2 billion in revenue annually.

The issue of spyware is no longer a case of cyber-scare—it's cyber-warfare. According to Frederick Feiman, senior vice-president of marketing for Tenebril, a security and privacy solutions company, "Spyware creators are constantly searching for techniques to evade anti-spyware vendors. Spyware creators are applying the techniques used by security software vendors and authors of viruses and Trojans to make their spyware more resilient."⁵

³ A virus is a self-replicating code that propagates by reproducing and inserting itself into other programs, documents, or e-mail attachments (Anti-Spyware Coalition, *Definitions and Supporting Documents*, July 2005).

⁴ FinFacts Team, *Spyware Generating Billions of Dollars: Report*, May 3, 2005, available at <www.finfacts.com>.



A Threat to Financial Institutions

Financial institutions are most concerned with the sophisticated array of spyware programs that can be used to track keystrokes, scan files, capture account names, confiscate passwords, and cause general confusion. For financial institutions that rely on the Internet to generate new business, this is a troubling development that has far-reaching effects on the banking industry. A recent Gartner Report noted that theft from personal bank accounts, where account numbers and passwords were stolen, was the fastest-growing type of financial fraud. Unfortunately, IT professionals say that many

company executives do not understand spyware's destructive potential.

Ways to Combat Spyware

The Federal Financial Institutions Examination Council (FFIEC) recommends that financial institutions take a layered security approach for effective risk mitigation. This includes:

- Implementing acceptable policies for non-work related browsing and software installation

continued on page 10

⁵ Jack Germain, "First State of Spyware Report Shows Bad Guys Winning," *TechNewsWorld*, May 11, 2005, available at <www.technewsworld.com>.

Authentication in an Internet Banking Environment

by William Lenney, Applications Analyst

While the proliferation of the Internet and electronic banking has provided bank customers with more flexibility and convenience, it has also meant new opportunities for increased criminal activity, including identity theft, account fraud, and money laundering. These threats have created an environment in which financial institutions must establish policies and procedures to safeguard customer information and to verify the identities of new customers.

Financial institutions engaging in Internet banking must have adequate controls to ensure effective and reliable methods for authenticating customer accounts in order to prevent money laundering, terrorist financing, fraud, and identity theft. The potential risks of conducting business with unauthorized persons include financial loss and increased reputational risk due to the improper disclosure of personal information, data corruption, fraud, or unenforceable agreements.

The Federal Financial Institutions Examination Council (FFIEC) has issued new interagency guidance in SR Letter 05-19,¹ entitled *Authentication in an Internet Banking Environment*. The new guidance re-

places the FFIEC's *Authentication in an Electronic Banking Environment* issued in 2001, and it specifically addresses the need for risk-based assessments, security measures, and customer awareness to reliably authenticate customers using a financial institution's Internet-based services. The guidance is pertinent to both retail and commercial customers, and it should be used by financial institutions when evaluating and implementing authentication systems, whether in-house or via a service provider. Financial institutions are expected to conform to these guidelines by year-end 2006.

The FFIEC believes that single-factor authentication is not adequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

There are a variety of technologies and methodologies for financial institutions to use to authenticate customers. Existing authentication methodologies involve three basic factors: 1) something the user *knows* (e.g., password, PIN); 2) something the user *has* (e.g., ATM card, smart card); and 3) something the user *is* (e.g., biometric characteristics, such as a fingerprint). The FFIEC believes that single-factor authentication is not adequate for high-risk transactions involving access to customer information or the movement of funds to other parties. An example of a single-factor authentication method is a customer logging into an account by entering a password. Multifactor authentication methods provide a stronger level of control. For instance, an Automated Teller Machine (ATM) transaction, which requires physical control of the ATM card and a Personal Identification Number (PIN), is a multifactor authentication method.

¹ SR 05-19, *Interagency Guidance on Authentication in an Internet Banking Environment*, is available on the Board of Governors' website at <www.federalreserve.gov/boarddocs/srletter/2005/sr0519.htm>.



Risk Assessment

Financial institutions should begin with a risk assessment of their Internet banking systems, focusing on the sensitivity of customer information, type of accounts, transactional capabilities, and transaction volumes. The type of authentication process should correspond with the level of risk related to the information and transactions.

Account Origination and Customer Verification

Financial institutions need to have adequate controls in place to verify customer identities. Moreover, customer identity verification during account origination is required by Section 326 of the USA PATRIOT Act, and it is important for reducing identity theft, fraudulent account applications, and unenforceable account agreements and transactions.

Monitoring and Reporting

In addition to preventive controls, institutions should have detective controls that can determine whether there has been unauthorized access to computer systems and customer accounts and that can analyze customer accounts to identify suspicious activities. Also, financial institutions should report suspi-

cious activities to the appropriate regulatory and law enforcement agencies as required by the Bank Secrecy Act.

Customer Awareness

Financial institutions must continue their efforts to educate customers, because customer education is a key defense against fraud and identity theft. Financial institutions can use a variety of methods to evaluate their customer education efforts by tracking the number of clicks on information security websites, the number of direct mail communications, and the actual losses due to identity theft at the institution.

Conclusion

A financial institution engaging in Internet banking must have adequate policies, procedures, and controls to reliably authenticate customers accessing its Internet-based services to prevent money laundering, terrorist financing, fraud, and identity theft. Risk-based assessments, security measures to reliably authenticate banking resources via the Internet, and customer awareness must be included in an institution's arsenal of defense against unauthorized actions. □

SR Letter 06-1 Issued January 20, 2006

Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), together with federal banking regulators, released interagency guidance for banking organizations related to the sharing of Suspicious Activity Reports (SARs) with head offices and controlling companies. The guidance confirms the following:

- A U.S. branch or agency of a foreign bank may disclose a SAR to its head office outside the United States.
- A U.S. depository institution may disclose a SAR to controlling companies (as defined in the guidance), whether foreign or domestic.

The guidance does not address whether a banking organization may share a SAR with its affiliates other than a controlling company or head office, regardless of its geographic location. The guidance states that a banking organization should maintain appropriate arrangements for protecting the confidentiality of its SARs.

FinCEN has issued concurrent similar guidance for securities broker-dealers, futures commission merchants, and commodities brokers.

A Look Back at 2005 and Expectations for 2006 ...continued from page 1

by Mike Collins, Senior Vice President

2005 to provide further information and clarification in certain identified implementation areas to help reduce any unnecessary costs and other burdens without jeopardizing the benefits of the new requirements. Moreover, outside auditors with experience from the previous year will likely make adjustments to improve the value of the process in 2006.

Management needs to keep current on all auditing and accounting issues to ensure that financial statements are prepared according to generally accepted accounting principles and to state financial results accurately. Last year, closure was reached on the Other-Than-Temporary Impairment guidance with the release of FASB Staff Positions (FSP) 115-1 and 124-1. The FSPs maintain the three-step process for determining investment impairment and nullify certain requirements of the original EITF 03-1. In 2006, updated FASB guidance related to business combinations and consolidated financial statements is expected to be finalized. One of the major issues is the elimination of the ability to carry over the allowance for loan and lease losses (ALLL) in a business combination. Also in 2006, final guidance is expected, amending FAS 140, *Accounting for Transfers and Servicing of Financial Assets and Extinguishment of Liabilities*, which deals with the issues of legal isolation and other conditions for sale treatment. In addition, accounting for post-retirement benefits will receive FASB's attention in 2006, and FASB is also expected to release draft guidance that addresses fair value accounting. Finally, the SEC will address disclosures surrounding executive compensation.

Compliance Risk

Compliance risk will remain a central focus for management in 2006. High-profile regulations were in the spotlight in 2005, including HMDA and the Bank Secrecy Act and Anti-Money Laundering (BSA/AML) rules. In today's climate of increasing organization complexity and business line diversity, organizations are strongly encouraged to manage compliance in a more integrated, enterprisewide manner. This allows them to identify potential gaps, overlaps, or unclear boundaries between their individual compliance programs and to help allocate resources to areas with higher reputational risk. While effective compliance risk management

In today's climate of increasing organization complexity and business line diversity, organizations are strongly encouraged to manage compliance in a more integrated, enterprisewide manner.

is imperative, it is important that banking organizations do not maintain a singular focus on compliance. Strategy, innovation, leadership, and growth are also key components for a successful organization.

Last year was the first year for the release of expanded HMDA data. The data alone are not a definitive indicator of unfair practices or lender abuses. Rather, the inclusion of loan pricing information provides regulators with a screening tool to identify situations where additional testing may be necessary to determine the effectiveness of fair lending compliance.

As planned, a new BSA/AML examination manual was released in June 2005. The new manual was designed to clarify existing regulatory requirements and examination expectations and to promote examination consistency among the regulators. It does not introduce any new guidance. Sound BSA/AML risk management enables an organization to identify risks, to better direct resources to safeguard op-

erations from money laundering or terrorist financing, and to ensure compliance.

Credit Risk

Throughout 2005, asset quality indicators showed no significant signs of deterioration, and underwriting standards were considered to be at historic highs, but strong competition can force easing of standards, and risk management practices may not have kept pace with the recent strong loan growth. High growth markets and increased commercial real estate (CRE) lending at community banks are two areas of current supervisory concern, and regulators are carefully monitoring CRE concentrations. In addition, strong growth in nontraditional mortgage products prompted the issuance of draft interagency guidance in late 2005. Regulators have concerns over the suitability of these products to a broader range of customers, the effect of payment shocks, and the layering of risk.

Interagency draft guidance on CRE concentrations was also released recently. Management must ensure that credit concentrations are monitored and managed effectively to limit risk exposure, and institutions with concentrations are expected to adopt advanced risk management practices to mitigate the associated risks. Now is an appropriate time to review lending manuals and the portfolio management process.

Also, in late 2005, loan loss provisions were on the rise. In 2006, close attention will be paid to this trend to determine whether this was only in response to one-time events or whether this supports indications that we have reached a peak in the credit cycle.

Interest Rate Risk

The Federal Open Market Committee raised its target for the fed funds rate eight times in 2005, bringing the total number of rate increases to 13 over the last 19 months. However, despite the ongoing increases in short-term rates, long-term rates were little changed. Accordingly, the yield curve continued to flatten in 2005, resulting in margin compression. Loan pricing did improve late in the year and, combined with solid loan growth, did offer minimal margin relief. Some



institutions have restructured their balance sheets in response to rising rates, and this has come at a cost. Regulators continue to express concern over leverage programs that are not effectively utilized, which can increase interest rate risk and create the potential for a negative impact on earnings in a rising rate environment. Another area of ongoing focus will be rising noncore funding levels as strong competition for deposits continues. In addition, continued margin pressure may lead to yield chasing, and unrealized securities losses have re-emerged as a result of the rate increases. Management should ensure that interest rate management practices remain strong through this evolving economic environment.

Mergers and Acquisitions

As was predicted in 2005, earnings growth is again expected to slow in 2006. There was strong merger activity in 2005, but it was less than in the previous year, and the total assets involved were greatly reduced. Due to the slowdown in earnings performance, a desire for continued growth and expansion, and a reduction in merger premiums, a renewed motivation for consolidation may emerge in 2006. Merger activity will be spurred by balance sheet mismatches, market share penetration strategies, management succession, equity prices, and rising expenses. New organizational infrastructures are also emerging in response to new technologies, market changes, and regulation. Nevertheless, de novo institutions will continue to form in response to consolidation.

Information Security

Incidents of threats to the security of customer information are in the news every day—phishing, hacking, insider abuse, and the loss of backup tapes. Regulators continue to focus on organizations' preventative measures for safeguarding customer information. In 2005, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information & Customer Notice* and *Interagency Guidance on Authentication in an Internet Banking Environment* were both issued. Due to the rapid changes in the business environment, management must be diligent in addressing its information security risks. This includes ensuring a secure relationship with third-party vendors when information technology is outsourced, including conducting due diligence of the vendor, assessing all of the associated risks, and completing regular reviews of practices and procedures supported by the vendor's products and services. Banking organizations are expected to design an information security program to control risks commensurate with the sensitivity of information and the complexity and scope of activities.

Ethics—Code of Conduct

The greatest risk to a firm's reputation is a breach of the law or its code of conduct. Banks should ensure that sound tenets of corporate governance are deeply rooted in their cultures to strongly promote and support an environment of ethical decision making.

Banks should ensure that sound tenets of corporate governance are deeply rooted in their cultures to strongly promote and support an environment of ethical decision making.

Business Continuity

Business impact and risk assessments are the foundation for an effective business continuity plan. Planning should be conducted on an enterprisewide basis, and plan effectiveness should be tested. Results should be subject to an independent audit and reviewed by the board of directors. Periodic updates are also necessary to address any changes in the organization or its service provider.

Competition for Talent

The ongoing shift to technologically-intensive industries, demographic shifts, and increasing competition for skilled lenders and risk managers may constrain an institution's ability to grow. A shortage of suitable candidates will require banking organizations to seek creative ways to deploy flexible staff and place a premium on effective recruitment and staff development and retention.

Basel II

Finally, no review of the past year or discussion of expectations for the coming year would be complete without a mention of the ongoing implementation of the proposed Basel II guidance.

The U.S. is striving to implement

the proposed international regulatory framework of Basel II by 2009. Establishing the link between regulatory capital and risk management and the need to identify and measure risk at the largest, most complex organizations are two of the key goals of the Basel II framework. A Basel I ANPR was issued in 2005 to address areas that are in need of updating and specific potential competitive implications of Basel II. □

Visit the **Federal Reserve System Publications Catalog** at www.newyorkfed.org/publications/frame1.cfm for all of your public information needs. A wide variety of materials are available for students, teachers, and the general public. Orders can be placed online for printed publications, and most documents can also be viewed online. Subscription service is available for certain publications.

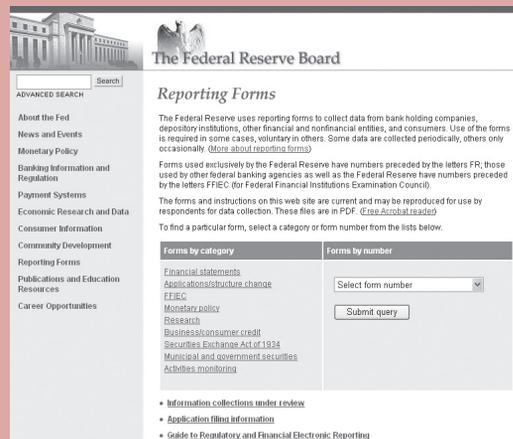
Check out FR Y-10 Online!

FR Y-10 Online is the electronic alternative for submitting the FR Y-10, *Report of Changes in Organizational Structure*, to the Federal Reserve. The FR Y-10 is filed to report mergers, changes to company characteristics, and changes in reportable investment activities.

Online filing has the following advantages:

- Immediate submission makes reporting deadlines easier to meet.
- Reports can be saved in draft form, allowing for editing and modifying prior to submission.
- Multiple access levels help control report modification and final submission.
- Sample reports are provided for guidance on entering data.

Security features include a unique user ID and an eight-character password. To begin using FR Y-10 Online or to learn more about required filing of the FR Y-10, visit www.federalreserve.gov/boarddocs/reportforms/default.cfm, and select the form number FR Y-10.



Introducing the New FR Y-10S Regulatory Report

The new FR Y-10S, *Supplement to the Report of Changes in Organizational Structure*, has two schedules. Schedule A collects information regarding the requirements to file annual and other periodic reports with the Securities and Exchange Commission (SEC), pursuant to Sections 13(a) or 15(d) of the Securities and Exchange Act, and regarding whether or not an entity must comply with Section 404 of the Sarbanes-Oxley Act. This schedule is filed annually, as of December 31, with the data due on March 1 of the following year.

Schedule B collects Committee on Uniform Securities Identification Procedures (CUSIP) information and is required as of December 31, 2005, initially. Going forward, Schedule B will be required on an event-generated basis. The initial date for filing Schedule B data is March 31, 2006.

The forms and instructions, including information on who is required to file, are located on the Board of Governors' website at www.federalreserve.gov/boarddocs/reportforms/default.cfm.

Please Note: The current version of the FR Y-10S cannot be submitted using FR Y-10 online at this time.

For more information on the FR Y-10S, please contact Financial Institution Structure (FIS) Supervisor Linda Booker (linda.booker@phil.frb.org) at 215-574-6051, FIS Analyst Artia Benjamin (artia.benjamin@phil.frb.org) at 215-574-6407, or FIS Analyst Josephine Brookins (josephine.brookins@phil.frb.org) 215-574-4345.

Spyware: A Hidden Danger for Financial Institutions

...continued from page 3

- Performing a regular assessment to verify that controls are effective and performing as intended
- Putting security monitoring in place for firewall and internal diagnostic system to analyze traffic for perceived or actual attacks
- Ensuring that licensing agreements are carefully read and peer-to-peer file sharing is avoided

In addition to the FFIEC recommendations, financial institutions can take several other steps to defend against persistent and damaging spyware and adware attacks:

- Enforce a no-download policy that discourages users from opening suspicious e-mails and attachments.
- Ignore pop-ups so that spyware/adware cannot be downloaded.
- Use only well-recognized and approved spyware tools; however, since no single solution prevents adware and spyware, it is best to consider using multiple utilities.
- Avoid fake anti-spyware tools offered on the Internet.
- Allow IT professionals to fix suspected adware or spyware problems—users should not attempt to fix their own systems.
- Lock down all browsers.
- Use an alternative browser to Internet Explorer, which is the most widely exploited browser on the Internet. Many other browser alternatives are just as fast, mature, and robust.
- Download system updates when available to keep your system safe and secure.

The Federal Deposit Insurance Corporation (FDIC) has advised banks to reduce online fraud by upgrading existing single-factor authentication systems

The FDIC has advised banks to reduce online fraud by upgrading existing single-factor authentication systems to two-factor authentication.

(password) to two-factor authentication.⁶ Two-factor authentication involves a password (something the user knows) and a smart card or token (something the user possesses). It could also involve biometrics, which are automated methods used to identify a person based on physiological or behavioral characteristics. In the U.S., eTrade, US Bancorp, and Bank of America have already announced plans to provide authentication tokens to corporate customers.

In October 2005, the FFIEC issued updated guidance entitled *Authentication in an Electronic Banking Environment* to support greater risk management controls for Internet-based financial services. The updated guidance stresses the need for financial

institutions to conduct risk-based assessments, implement robust customer authentication measures, and evaluate customer awareness programs.⁷

In its study, *Putting an End to Account-Hijacking Identity Theft*, the FDIC made the following additional recommendations for protecting consumer information online:

- Financial institutions must share the responsibility of educating their customers regarding the potential hazards of online scams.

⁶ Federal Deposit Insurance Corporation, *Putting an End to Account-Hijacking Identity Theft*, December 14, 2004, available online at <www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf>.

⁷ Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment*, October 12, 2005, available online at <www.ffiec.gov/press/pr101205.htm>.

- New technologies must be encouraged to help protect financial institutions and consumers from such threats.
- The technology and financial services industries, along with the government, must foster the sharing of information on defensive technologies.⁸

Financial institutions are also in ongoing discussions with consumer groups and government agencies concerning who should pay for losses associated with spyware attacks. No consensus has emerged on this issue; however, some banking industry analysts have called on banks to follow the model established by credit card companies—where the financial institution is liable for all but the first \$50 of fraudulent transactions. However, if two-factor authentication standards are adopted industrywide, an increasing share of the burden may be placed upon the online customer.

Legislative Responses

In the Third Federal Reserve District, legislation was introduced on February 16, 2005, by Pennsylvania State Representative Victor John Lescovitz (D-Allegheny County) to combat the pervasive threat of spyware. The proposed bill (H.B. 574) would amend Title 18 (Crimes and Offenses) of the Consolidated Pennsylvania Statutes, making it illegal “to use a computer or computer network without authority and with the intent to falsify or forge electronic mail transmission information or other routine information in any manner in connection with the transmission of unsolicited electronic mail through or into the computer network of an electronic mail service provider, Internet service provider or its subscribers.” Fines for violations of the proposed law would range between \$2,500 and

⁸ Federal Deposit Insurance Corporation, *Putting an End to Account-Hijacking Identity Theft*, December 14, 2004, available on line at <www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf>.



\$15,000, depending upon the damage inflicted from the assault. The bill has been referred to the House Committee on the Judiciary for consideration.

A summary of current efforts to control the proliferation of spyware and adware for all 50 states can be found at <www.benedelman.org/spyware/legislation/>.

Fines for violations of the proposed law would range between \$2,500 and \$15,000, depending upon the damage inflicted from the assault.

An End to Spying

Positive signs in the fight against Internet fraud have emerged. The 2005 e-Readiness Rankings, a white paper released in April 2005 by the Economist Intelligence Unit and written in cooperation with the IBM Institute for Business Value, ranked the United States second in its survey of 65 countries for its e-readiness.⁹ Indeed, this is a positive sign that corporate Amer-

ica is taking steps to combat emerging cyber threats, such as spyware, which pose serious obstacles to a vibrant e-commerce environment. The U.N. Conference on Trade and Development estimated that nearly \$600 billion will be spent on IT-related outsourcing in 2005. With this type of investment, organizations must continue to fight fraudulent activity like spyware. □

⁹ Economist Intelligence Unit, *The 2005 e-Readiness Rankings*, 30 April 2005.



FEDERAL RESERVE BANK
OF PHILADELPHIA

Supervision, Regulation and Credit Department
Ten Independence Mall
Philadelphia, PA 19106

www.philadelphiafed.org

E-Mail Notification Service

Would you like to read *SRC Insights* and *Compliance Corner* on our website 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.