

# Insights

FEDERAL RESERVE BANK OF PHILADELPHIA

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

Volume 6 Issue 1

## IN THIS ISSUE

SVP Commentary ..... 1

COSO: What Does it Mean for Bank Supervision? ..... 2

Keeping Trust Honest: Supervising Fiduciary Activities ..... 4

Compliance Corner ..... CC1

Feeling a Little Lost? ..... 8

E-Mail Notification Service ... 8

## CIRCULATE TO:

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

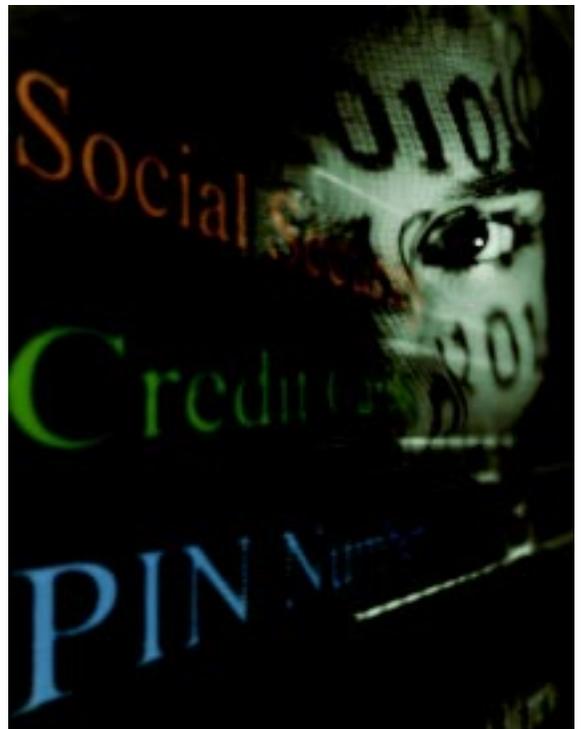
### SVP Commentary on...

## The New IT – “Identity Theft”

by Michael E. Collins

Throughout the late 1990’s, the two letters on the tip of everyone’s tongue were “IT” – Information Technology. Today, these two letters retain their prominence, but for another reason – Identity Theft. Identity theft is not a new problem. However, the increasing sophistication and broader distribution of technology, while providing numerous benefits, have also facilitated the theft and fraudulent use of personal information.

Identify theft, the fraudulent use of an individual’s personal identifying information, is a growing problem. From November 1999 through May 2001, the Federal Trade Commission processed over 85,000 entries to its Identity Theft Hotline and Data Clearinghouse.<sup>1</sup> Of these entries, 70 percent were victims reporting incidents in which one or more types of identity theft occurred. The remaining entries were consumer requests for information on identity theft and consumer reports of suspicious activities that had not yet led to identity theft.



<sup>1</sup> See the FTC’s report, *Identity Theft Complaint Data*, and the related PowerPoint slides at <[www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/)>.

*continued on page 6*

# COSO:

## What Does it Mean for Bank Supervision?

by John J. Deibel, Vice President

COSO, The Committee of Sponsoring Organizations of the Treadway Commission, is a voluntary, private sector group of organizations that is dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and

vision (“the Basel Committee”) incorporated the COSO guidance when issuing its *Framework for Internal Control Systems in Banking Organisations*.<sup>3</sup> The Basel Committee’s framework applies the COSO principles to banking organizations and is designed to

When preparing its study, the Basel Committee studied control breakdowns in each of the five components. It noted that breakdowns in these components led to significant losses in banking organizations, and that these losses might have been

### Internal control is not a single event or activity, but should be the underlying foundation within an organization.

corporate governance.<sup>1</sup> COSO is perhaps best known for its September 1992 study, *Internal Control – Integrated Framework*. This study quickly became the definitive guidance for organizations seeking to improve their internal control environment. As one of COSO’s sponsoring organizations, the American Institute of CPAs (AICPA) incorporated this guidance into its generally accepted auditing standards.<sup>2</sup>

Of more relevance to the banking industry, in September 1998 the Basel Committee on Banking Super-

be used by bank supervisors worldwide when evaluating banks’ internal control systems.

As defined by COSO, internal control is a process designed to provide reasonable assurance regarding (i) the effectiveness and efficiency of operations, (ii) the reliability of financial reporting, and (iii) compliance with applicable laws and regulations. By defining internal control as a process, COSO acknowledged that internal control is not a single event or activity, but should be the underlying foundation within an organization. Both COSO and the Basel Committee note that internal control is comprised of five interrelated components: the control environment, risk assessment, control activities, information and communication, and monitoring (see sidebar on page 3). These components are most effective when they operate as a dynamic system, and not as individual silos of activity.

avoided if effective internal control systems had been in place. The Basel Committee reiterated that sound internal controls are essential and provide the foundation for the prudent operating of the banking system.

While the Federal Reserve System has not directly incorporated the entire COSO framework into its supervisory processes, many elements from the framework are included in the internal control procedures in the *Commercial Bank Examination Manual*.<sup>4</sup> In addition, implementation of the COSO framework in the banking industry has had a direct impact on the scope of our supervisory activities.

Over the past several years, the Fed-

---

<sup>1</sup> See COSO’s website at <[www.coso.org](http://www.coso.org)>.

<sup>2</sup> See the AICPA’s Statement on Auditing Standards No. 78, *Consideration of Internal Control in a Financial Statement Audit*.

<sup>3</sup> See *Framework for Internal Control Systems in Banking Organisations* at <[www.bis.org/publ/bcb40.pdf](http://www.bis.org/publ/bcb40.pdf)>.

---

<sup>4</sup> See section 1010 of the *Commercial Bank Examination Manual* at <[www.federalreserve.gov/boarddocs/supmanual/](http://www.federalreserve.gov/boarddocs/supmanual/)>.

eral Reserve has enhanced its supervisory processes for examinations and inspections of state member banks, bank holding companies, and U.S. branches and agencies of foreign banking organizations (FBOs). Effective planning and scoping are now emphasized in order to customize examinations and inspections to suit the size and complexity of the activities being reviewed and to concentrate limited examiner resources on areas that pose the greatest risk. As part of this risk-focused process, examiners direct more attention to evaluating internal risk management processes, including internal controls, to determine the degree of required transaction testing.

All organizations, regardless of size or complexity, should have effective internal control systems. However, smaller and less complex organizations may implement the components of internal control differently than larger and more complex organizations. Federal Reserve examiners carefully consider the nature and structure of the organization when assessing risk management processes and internal controls. Based on this assessment and the on-site and off-site examination and inspection activities, examiners assign banks and bank holding companies, except small shell bank holding companies, a risk management rating.<sup>5</sup> This rating is a significant part of the examiner's evaluation of the manage-

ment components of CAMELS (state member banks), BOPEC (bank holding companies), and ROCA (FBOs).

Experience has shown that sound risk management systems, including internal controls, will reduce the amount of transaction testing and permit greater reliance on the work performed by internal and external au-

ditors and outside consultants or accounting firms. Accordingly, the COSO framework is an integral part of the supervisory emphasis of the Federal Reserve Bank of Philadelphia, and, when effectively implemented, it will help to improve supervisory effectiveness and reduce regulatory burden to the industry. ■

## COSO's Five Components of Internal Control

**Control Environment:** The control environment sets the tone for the entire organization. It includes the integrity, ethical values, and competence of all people within the organization, including staff, management, and the board of directors. The control environment is the foundation for all of the other components.

**Risk Assessment:** An organization must be aware of the internal and external risks that could prevent it from attaining its objectives. The risk assessment should also include implementation of mechanisms to identify, analyze, and manage risks.

**Control Activities:** Control activities encompass the policies and procedures that are established and implemented to ensure that identified risks are managed and the organization's objectives are carried out. Control activities should occur throughout all levels of the organization.

**Information and Communication:** Information and communication, both internal and external, should be timely and flow in all directions within the organization. Effective information and communication systems allow an organization and its people to conduct, manage, and control operations and mitigate risks.

**Monitoring:** The entire control process must be monitored through ongoing and periodic reviews of the control system. Internal control deficiencies should be appropriately reported. When necessary, organizations should modify the control systems to ensure the organization can continue to react appropriately in a dynamic environment.

---

<sup>5</sup> See SR 95-51, *Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies*, at <[www.federalreserve.gov/boarddocs/srletters/1995/sr9551.htm](http://www.federalreserve.gov/boarddocs/srletters/1995/sr9551.htm)>.

# Keeping Trust Honest: Supervising Fiduciary Activities

by James W. Corkery, Examiner

If you want to make a banker smile, simply discuss the millions of dollars of fee income being generated by fiduciary activities. An established and well run trust department can provide significant returns to an organization's bottom line. On the other hand, mention the supervisory aspects of fiduciary activities, and you'll see bankers cringe.

To help alleviate concern and provide bankers with a better understanding of the fiduciary examination process, this article will focus on fiduciary examination frequency mandates, the rationale behind supervisory risk assessments, and the elements of a sound risk management program, all from the perspective of the Federal Reserve System.

## Examination Frequency Mandates

How do examiners know when to come for a visit? Before 2001, frequency mandates for trust examinations were based primarily on the size of an institution's fiduciary operations and its most recent examination rating. Effective February 2001, SR 01-5, *Examination of Fiduciary Activities*, established new guidelines for the frequency and scope of fiduciary examination activities of state-chartered member banks.<sup>1</sup> The purpose of SR 01-5 is to foster the integration of the assessment of fiduciary activities with the overall safety and soundness supervision process.

The examination frequency for complex fiduciary organizations—which

include large complex banking organizations (LCBOs), other large or regional institutions, and clearing agencies registered with the SEC—should be determined based on the impact of fiduciary activities on the organization's risk profile. Minimally, all material business lines should be examined over a two-year period, with higher risk areas generally reviewed annually.

In general, smaller state-chartered member banks and trust companies with non-complex operations should be reviewed no less frequently than during every other routine safety and soundness examination. Institutions not subject to routine examination should have an examination of their fiduciary activities conducted no less frequently than every two years.

In those instances where supervisory concerns have been cited, an additional level of supervisory attention is warranted. The examination frequency will be adjusted based on the severity of the supervisory concern, and action will be initiated and continued until all of the deficiencies have been addressed.

As indicated above, the frequency of examinations is primarily driven by the risk assessment process. By now, most bankers are thinking, "If I know what the regulators are looking at, maybe I can extend the time between supervisory visits." So what do the examiners look for in assessing fiduciary risk?

## Supervisory Assessments of Fiduciary Risk

In aligning fiduciary examinations

with safety and soundness risk assessments, fiduciary examiners prepare formal risk profiles of fiduciary activities for internal use by SRC staff. The frequency of these assessments depends on the size and complexity of the organization. For LCBOs, risk profiles will be updated quarterly with explicit consideration given to the risks of fiduciary activities. For other complex organizations, risk profiles will be prepared and updated at least annually. Risk assessments for smaller, non-complex organizations should be updated at each examination and incorporated into supervisory plans.

Based on the profile of the Third Federal Reserve District and our usual practice of interacting with trust institutions on a regular basis, this Reserve Bank updates trust-related risk profiles on a semi-annual basis. The updating process normally consists of a telephone conversation that, in some instances, may also involve a request for copies of written information.

As detailed in SR 01-5, the following factors would normally be reviewed:

- Size and number of fiduciary accounts and assets administered
- Nature and complexity of fiduciary products and services offered
- Changes to management and staffing
- Changes to data processing systems
- New affiliations, partnerships, or outsourcing arrangements
- Changes in strategic direction or exposure to emerging risks

<sup>1</sup> See SR 01-5, *Examination of Fiduciary Activities*, at <[www.federalreserve.gov/boarddocs/SRLETTERS/2001/SR0105.HTM](http://www.federalreserve.gov/boarddocs/SRLETTERS/2001/SR0105.HTM)>.

- Significant litigation, settlements, or charge-offs
- Scope and length of time since last on-site examination
- Significance of prior examination findings
- Effectiveness of the control environment, including audit and risk management practices.

## Elements of Sound Risk Management

The soundness of a bank's fiduciary risk management process also will help examiners determine the frequency of examinations. SR 96-10, *Risk-Focused Fiduciary Examinations*, provides guidance on the elements of a sound risk management program.<sup>2</sup> This SR Letter details four areas that should be considered in assessing the soundness of a bank's fiduciary risk management system. Accordingly, in assessing its risk management processes, an institution should consider the answers to the questions on the right.

With some of the mystery behind examination scheduling revealed, bankers can, to some degree, determine their own examination destiny by managing the risk profile of their fiduciary activities.

If you have any questions on issues related to fiduciary examinations, please contact your primary regulatory agency. For those institutions that are supervised by the Federal Reserve Bank of Philadelphia, please contact John Mendell, Team Manager, (john.mendell@phil.frb.org) at 215-574-4139. ■

<sup>2</sup> See SR 96-10, *Risk-Focused Fiduciary Examinations*, at <[www.federalreserve.gov/boarddocs/SRLETTERS/1996/SR9610.HTM](http://www.federalreserve.gov/boarddocs/SRLETTERS/1996/SR9610.HTM)>.

### *Active board and management oversight*

- ? Does the board and management have a clear understanding and knowledge of the activities performed and the risks inherent in those activities?
- ? Is management providing adequate supervision for daily activities?
- ? Does management identify fiduciary risk associated with new products and provide appropriate control over existing products?

### *Adequate policies, procedures, and limits*

- ? Do policies and procedures adequately address the fiduciary activities performed, and are they consistent with management experience and stated goals and objectives?
- ? Do the policies and procedures provide adequate identification, measurement, monitoring, and control of fiduciary risks?
- ? Are lines of authority and accountability clearly established?
- ? Do policies provide for the review of new fiduciary services, activities, and products prior to implementation?

### *Adequate risk monitoring and management information systems*

- ? Do fiduciary risk monitoring practices and reports encompass all business lines and activities?
- ? Are key assumptions, data sources, and procedures appropriate, adequately documented, and tested for reliability?
- ? Are reports to management accurate and timely, and do they contain sufficient information for decision makers to evaluate the level of risk?

### *Comprehensive internal control environment*

- ? Are internal controls appropriate for the level of fiduciary activity?
- ? Is the organizational structure adequate and are reporting lines sufficient for control?
- ? Are financial, operational, and regulatory reports reliable, accurate, and timely?
- ? Are internal audit and other control practices independent and objective, tested and reviewed, and presented to directors on a regular basis?

# COVER STORY

## “Identity Theft” continued from page 1

The growing problem of identity theft is also confirmed by the Suspicious Activity Reports (SARs) filed by financial institutions. The Financial Crimes Enforcement Network (FinCEN) has reported that, from April 1996 through November 2000, 1,030 SARs included reports of identity theft.<sup>2</sup> Of particular note is that the frequency of SAR filings for identity theft increased from an average of four per month in 1997 to over fifty per month in 2000.

As thousands of Americans are learning, identity theft is not something that happens to “the other guy.” The

was 40 years of age, with over 76 percent of the victims ranging from 18 to 49 years of age. In addition, approximately 12 percent of the victims reporting identity theft to the FTC had a personal relationship with the suspect, whether as a family member; a roommate; a co-worker, employer, or employee; a neighbor; or another unspecified relationship.

As one would expect, most of the identity theft schemes also affected depository institutions. Over 45 percent of the FTC identity theft complaints involved credit card fraud — opening a new account in the name

FinCEN report include depositing fraudulent, worthless, or counterfeit checks into an account and withdrawing funds before the checks cleared; obtaining loans to purchase high-end automobiles; and intercepting bank checks or convenience checks issued by credit card companies from the victim’s mail. Submitting fraudulent change of address forms, obtaining new checks, and receiving the victim’s bank statements were other means of committing identity theft.

Given the importance of trust and confidence to the banking system, depository institutions obviously have an interest and a role in preventing identity theft. First, there is the depository institution’s moral and legal obligation to protect its customers’ personal information. Indeed, because of the personal and confidential nature of the information exchanged between a depository institution and its customers, depository institutions are required by law and regulation to take appropriate measures to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information. Second, there is the depository institution’s obligation to its shareholders and to taxpayers to take necessary steps to minimize losses related to fraud.

Some believe that a proactive approach by depository institutions is key to preventing identity theft. At a March 2000 National Summit on

**Over 45 percent of the FTC identity theft complaints involved credit card fraud — opening a new account in the name of the victim or making unauthorized charges on an existing account.**

FTC has received complaints from consumers in all fifty states and the District of Columbia, while FinCEN has received SARs from 194 institutions in 41 states and the District of Columbia. The average consumer reporting identity theft to the FTC

of the victim or making unauthorized charges on an existing account. Approximately 14 percent reported bank fraud, where a new bank account was opened in their name and/or fraudulent checks were written or unauthorized withdrawals were made from an existing account. Eight percent of the victims reported that fraudulent loans were obtained in their name.

Common schemes cited in the

---

<sup>2</sup> See FinCEN’s report, *The SAR Activity Review: Trends, Tips & Issues*, at [www.treas.gov/fincen/](http://www.treas.gov/fincen/).

Identity Theft, Beth Givens, director of the Privacy Rights Clearinghouse, observed that while consumers can take precautions to minimize the risk of identity theft there is little they can do to prevent it. Rather, Ms. Givens believes the key is for businesses to establish responsible information-handling practices and for the credit industry to adopt stricter application verification procedures.

On April 26, 2001, the Federal Reserve System issued SR 01-11, *Identity Theft and Pretext Calling*.<sup>3</sup> Consistent with the requirements in section 525 of the Gramm-Leach-Bliley Act,

confidentiality, and integrity of customer information.

As discussed in the SR Letter and Interagency Guidelines, depository institutions can take various steps to protect customer information and reduce the risk of loss. Establishing and enforcing policies and procedures to verify the identity of individuals applying for financial products, including both deposits and loans, and establishing policies and procedures to prevent fraudulent activities related to customer information are two areas discussed in SR 01-11. Maintaining a sound information security pro-

Many depository institutions already have some or all of these recommended information security elements in place. However, all institutions should review and, if necessary, revise their information security policies, procedures, and practices to ensure that they are consistent with the Interagency Guidelines and SR 01-11. In accordance with the Interagency Guidelines, Federal Reserve safety and soundness examiners will review each institution's programs for safeguarding customer information and its compliance with the Interagency Guidelines on examinations starting after July 1, 2001.

## All institutions should review and, if necessary, revise their information security policies, procedures, and practices to ensure that they are consistent with the Interagency Guidelines and SR 01-11.

SR 01-11 provides guidance on protecting customer information, reporting suspected identity theft and pretext calling, and educating and assisting consumers. SR 01-11 also supplements guidance in the January 17, 2001 release, *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*.<sup>4</sup> These Interagency Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security,

program, the third element in the SR Letter, is more than policies and procedures. As described in detail in the Interagency Guidelines, development and implementation of an information security program includes the following elements:

- Board of Directors involvement
- Risk assessment
- Management and control of risk
  - Design of information security system
  - Training
  - Monitoring and testing key controls
- Oversight of service provider arrangements
- Modifications
- Board of Directors reporting

From a consumer's perspective, recovering from identity theft can be both costly and time consuming, and requires working with numerous third parties, including credit bureaus. Through this process, the consumer comes to view the villain as not just the individual who stole their identity, but the bureaucracy that prevents them from quickly restoring their good name. As I noted in the fourth quarter 1999 issue of *SRC Insights*, the single most valuable asset of financial institutions is the trust that their customers place in them. Through the diligent application of effective policies and procedures and the prompt reporting of suspicious activities, depository institutions will be able to more effectively deter identity theft and continue to maintain their customers' trust. ■

<sup>3</sup> See SR 01-11, *Identity Theft and Pretext Calling*, at <[www.federalreserve.gov/boarddocs/SRLETTERS/2001/sr0111.htm](http://www.federalreserve.gov/boarddocs/SRLETTERS/2001/sr0111.htm)>.

<sup>4</sup> See *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* at <[www.federalreserve.gov/boarddocs/press/boardacts/2001/20010117/default.htm](http://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010117/default.htm)>.

# Feeling a Little Lost?

Are you searching for an article from a recent issue of *SRC Insights*? Perhaps the on-line index of articles might be of help. Visit our web site at <[www.phil.frb.org/src/index.html](http://www.phil.frb.org/src/index.html)> to view current and past issues of *SRC Insights*, including recent articles such as the following.

- A Post-GLB Observation: Applications Might Still be Required for Non-Banking Activities (Q4 2000)
- A Regulatory Perspective on FHC Consolidated Supervision (Q4 2000)
- E-Sign Act Permits Electronic Delivery of Contracts, Signatures, Disclosures, and Records (Q2 2001)
- Reducing the Burden: New CRA and Compliance Examination Frequency for Small Banks (Q3 2000)
- Using Self-Evaluations to Streamline the Fair Lending Examination (Q1 2000)
- Internet Banking Examinations: Practical Guidelines (Q3 2000)
- Subprime Lending: New Definitions, New Guidelines (Q2 2001)
- Commercial Loan Underwriting: Balancing Competitive Pressures and Prudent Practices (Q1 2000)
- SVP Commentary on Liquidity Management (Q2 2001)
- SVP Commentary on Credit Risk in Today's Economy (Q4 2000)
- SVP Commentary on Predatory Lending (Q3 2000)



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.phil.frb.org](http://www.phil.frb.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.

## 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!

Send an e-mail to [cynthia.course@phil.frb.org](mailto:cynthia.course@phil.frb.org) to have your name added to the notification list.