



Insights

FEDERAL RESERVE BANK OF PHILADELPHIA

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

Volume 9 Issue 1

IN THIS ISSUE

SVP Commentary 1

Evolution and Trends in Suspicious Activity Report (SAR) Filings 2

Biometrics: A Viable Solution for Financial Institutions? 4

From BOPEC to RFI: A Change is Coming 14

Compliance Corner CC1

CIRCULATE TO:

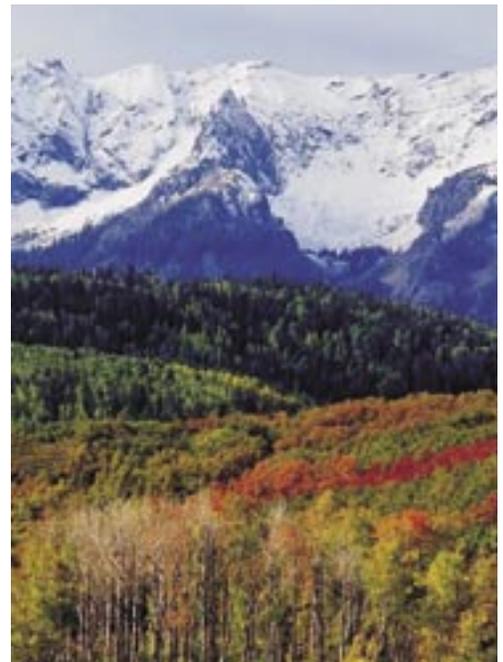
- _____
- _____
- _____
- _____

SVP Commentary on... The Changing Supervisory Landscape

The banking and financial services industry and the regulators responsible for its effective oversight are engaged in a major period of transformation. Several trends are responsible for this changing landscape, including process improvements aided by technology, new products and services, enhancements in risk management, international policy initiatives, increased complexity, and consolidation.

The ways that banking organizations monitor and manage exposures and activities have been facilitated by technology, advances in risk management, and improvement in internal processes. In turn, new products have emerged; financial services have converged; and banking, capital, and financial markets have advanced and become more sophisticated.

Banking industry consolidation has also been a transforming trend, concentrating assets and deposits among a few of the nation's largest financial institutions, creating national footprints and potentially changing the value proposition of



continued on page 9

Evolution and Trends in Suspicious Activity Report (SAR) Filings

by Frank J. Doto, Enforcement and Surveillance Officer and William J. Brown, Senior Examiner

The *Bank Secrecy Act* (BSA) was enacted in 1970, authorizing the Secretary of the Treasury to require financial institutions to keep records and file reports that the Secretary determined to have a high degree of usefulness in criminal, tax, or regulatory investigations. The BSA criminalized money laundering and placed reporting and record keeping requirements on financial institutions. The submissions of Currency Transaction Reports (CTRs), monitoring for suspicious activity, and the filing of Suspicious Activity Reports (SARs) have served as the foundation of the BSA.

The information presented in this article is meant to provide background on the evolution of the SAR program and context regarding the trends and volume of violations reported both nationally and in the tri-state area. This context may be helpful to financial institutions when reviewing program results, helping management determine if their experiences are aligned with the averages for their market areas.

SARs: The Basics

Effective April 1, 1996, the Suspicious Activity Report (SAR) replaced the Criminal Referral Form. A SAR must be filed with the Department of the Treasury under the following circumstances:

- Insider abuse involving any dollar amount that the financial institution detects or any known

or suspected federal criminal violation, committed or attempted against the institution when the suspect is a director, officer, employee, agent, or other institution-affiliated party.

In general, a SAR should identify the five basic elements of information – Who? What? When? Where? and Why?

- Violations aggregating \$5,000 or more in funds or other assets where a suspect can be identified.
- Violations aggregating \$25,000 or more in funds or other assets even though there is no substantial basis for identifying a possible suspect or group of suspects.
- Transactions aggregating \$5,000 or more that involve potential money laundering or violations of the BSA, or where the transaction has no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to engage, and

the bank knows of no reasonable explanation for the transaction after examining the available facts.

The information provided in a SAR provides the Treasury Department with a means to identify emerging trends and patterns associated with financial crimes. Accurate and timely information is critical to the law enforcement agencies, and financial institutions should ensure that SAR submissions are complete, sufficient, and timely.

In general, a SAR should identify the five basic elements of information – Who? What? When? Where? and Why? In essence, the following five questions should be answered when completing a SAR:

- **Who** is conducting the suspicious activity?
- **What** instruments or mechanisms were used to facilitate the suspicious transaction(s)?
- **When** did the suspicious activity take place?
- **Where** did the suspicious activity take place?
- **Why** does the SAR filer think the activity is suspicious?

In addition, the filer should use the narrative section of the SAR to answer the question, “How did the suspicious activity occur?” Any failure to adequately describe the factors that make the activity suspicious undermines the very purpose of the

SAR and lessens its usefulness to law enforcement.

The SAR should be filed with the Financial Crimes Enforcement Network (FinCEN), an office within the Department of the Treasury, in either hard copy or electronic form. The financial institution should maintain a copy of the SAR along with any supporting documentation for a period of five years from the date of filing. Bank management should notify its board of directors, or a committee thereof, of all SARs filed.

Supervisory action may be initiated against a financial institution, its board of directors, officers, employees, agents, or other institution-affiliated parties for a failure to file a SAR. The action could be in the form of a cease and desist order or civil money penalties.

Neither the filing nor the contents of the SAR may be disclosed to anyone outside the financial institution, with the exception of authorized law enforcement and regulatory authorities. This so-called safe harbor protection was recently reaffirmed in the federal court, and the highlights of the case were noted in the May 2004 SR Letter 04-8 *Interagency Advisory Concerning the Legal Protections Associated with the Filing of Suspicious Activity Reports*.¹

The USA PATRIOT Act and AML

Since the BSA was signed into law in 1970, it has been amended several

times. The most recent changes to the BSA came with the passage of the USA PATRIOT Act in October 2001. These amendments shifted the BSA's emphasis from record-keeping to a broader application of all-encompassing Anti-Money Laundering (AML) programs. The USA PATRIOT Act also extended AML requirements to other types of financial institutions previously not covered under the BSA. Currently, depository institutions, money service businesses, casinos and card clubs, and securities/broker dealers are required to have AML programs, and are required to file SARs.

The broader application of AML programs reflects Congress's realization that the U.S. financial system is an important instrument in identifying potential threats to our country. By using the primary AML reporting tool—the SAR—financial institutions can help identify the threat of terrorism, in addition to aiding in identifying other types of clandestine activities, such as organized crime, drug smuggling, and a number of other serious crimes.

SAR Trends

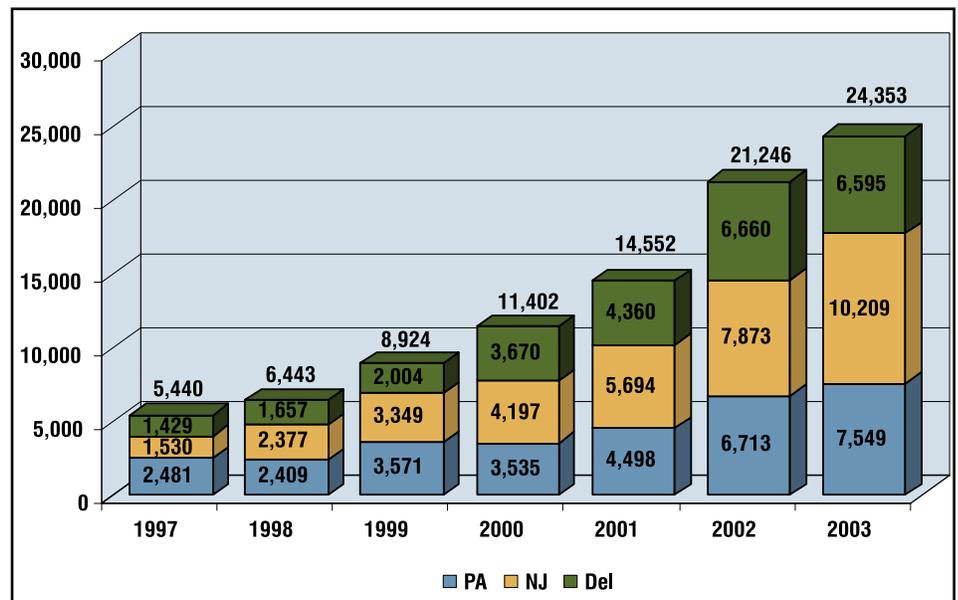
The Numbers. The number of SAR filings has increased dramatically over the years. In the past seven years, national SAR reporting increased 255 percent from 81,197 filings in calendar year 1997 to 288,343 filings in calendar year 2003.² From 2000 to 2003 alone, SAR filings increased 77 percent. As shown in Exhibit 1, the increasing filing trend in the tri-state area has been even greater, with 5,440 filings in 1997 and 24,353 filings in 2003. New Jersey leads the increase with 10,209, up from 1,530, and has recorded one of the highest percentage increases in the nation.

When aggregating all SAR filings by state from April 1996 through December 2003, California has the highest number of SAR filings,

² See FinCEN's *The SAR Activity Review by the Numbers*, Issue 2, May 2004 at <www.fincen.gov/bythenumbersissue2.pdf>.

continued on page 6

Exhibit 1. SAR Filings in the Tri-State Area



¹ SR Letter 04-8 is available on the Board of Governors' web site at <www.federalreserve.gov/boarddocs/SRLETTERS/2004/sr0408.htm>.

Biometrics: A Viable Solution for Financial Institutions?

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

Financial institutions and their customers may be closer than ever to living in a futuristic world driven by biometric technologies. Forget the virtual reality kiosk at your local shopping mall, not even motion picture director George Lucas could imagine biometric solutions like those now being developed by research laboratories nationwide. With considerable advancements realized over the past twenty years, an astonishing array of biometric solutions are now available to financial institutions seeking customized products to meet their physical security, computer access, and data management needs.

Traditional security approaches used by financial institutions normally focus on locks and keys, numeric keypads, magnetic cards/PINs, usernames/passwords, surveillance cameras, and human guards. These security approaches, while somewhat effective, have clear limitations. Keys and passwords are often lost, stolen, or damaged. PINs are designed to identify a card and password, but not the user. Surveillance cameras are susceptible to malfunction, disrepair, and quality issues. Human guards are expensive and prone to error.

Used independently or to supplement existing security measures such as smart cards, biometric technologies offer financial institutions legitimate alternatives to protect against illicit criminal activity, such as identity theft, account manipulation, and fraud. Identity theft, in particular,

has become an increasing threat to the autonomy and independence of financial institutions. A recent survey released by Dr. Alan Westin, Professor Emeritus of Public Law and Government at Columbia University, showed 33.4 million Americans have been the victims of fraud or identity theft since 1990, with 13 million cases since 2001.¹ The same survey noted that since 2001, out-of-pocket expenses for victims have totaled \$1.5 billion annually.

The International Biometric Group, a biometric consulting and technology services firm, recently released its Biometric Market Report for 2003-2007.² Some of report's more notable findings include:

- Global biometric industry revenues, which stood at \$601 million in 2002, are expected to reach \$4 billion by 2007.
- The largest increase in revenue will occur in fingerprint-based technologies.
- Facial-Scan and Middleware biometric technology revenues are expected to reach \$200 million and \$215 million respectively by 2007.

- The government sector will continue to be an attractive market for biometric technologies, generating \$1.2 billion in expected annual revenues through 2007. The financial sector will account for \$672 million in annual revenues, while travel and transportation will account for an additional \$556 million in annual revenues through 2007.

This article will examine biometrics as an alternative to current authentication and verification measures. It will review the functionality of biometric devices, describing the various types of biometrics now available to financial institutions and providing examples of current business and government uses; review broader legislative and regulatory action; discuss the evolving market for biometrics, including at financial institutions; outline recent Federal Reserve action; and provide general conclusions.

What are Biometrics?

In our everyday lives, most identification occurs through our personal interaction with others. If this identification method is unavailable, the next best alternative involves the introduction of "tokens." Tokens come in two forms: *knowledge tokens*, which include passwords, PINs, or personal data, and *physical tokens*, which include identification cards, chip cards, passports, and keys. Knowledge and physical tokens have worked well in the past in reducing identity theft and fraud because they can be revoked or

¹ See the *Biometric Digest*, September 2003, at <www.biodigest.com>.

² See The International Biometric Group's web site at <www.biometricgroup.com/index.html>.

reissued. However, like most mature technologies, cracks have appeared in the armor, as fraudsters have found ways to compromise authentication, identification, and verification measures.

This brings us to the next generation of security products for financial institutions—biometrics. The term “biometrics” refers to automated methods used to identify a person based on physiological or behavioral characteristics.³ *Physiological Biometrics* are based upon data resulting from the direct measurement of a part of the human body, such as hand geometry, finger images, facial characteristics, voice, and iris recognition. *Behavioral Biometrics* are based on an action taken by a person; they are traits that

system using a fingerprint scanner. The system performs a check against a database containing authorized individuals to determine if the sample on file matches the sample presented.⁴ This identification system reduces the probability of more than one individual using an identity.

In a *negative identification* scenario, an individual claims not to be someone already registered in a system’s database. The system checks the database to affirm that the individual is not on a “watch list” of individuals.⁵ This watch list may include bank robbery suspects, credit card or identity theft fraudsters, or individuals suspected of other criminal activities.

Biometrics are used by a growing

security, including Barclays and Barclays Card, UBS, American Express, Bank of Montreal, Westdeutsche Landesbank, Bank of Nova Scotia, Bear Stearns, Prudential, Bank of Slovenia, Union Bank of California, and Morgan Stanley. In practice, fingerprinting takes an ink or digital scan image of an individual’s fingertips and records unique features such as whorls, arches, ridge patterns, loops, furrow patterns, and other details. This information is stored as an image or as an encoded computer algorithm and is compared to an existing database for identification or verification. An advantage of this technology is that fingerprints are difficult to counterfeit, given the intricate information in each fingerprint. For depository institutions, the use of fingerprint biometrics could provide a

For depository institutions, the use of fingerprint biometrics could provide a more secure alternative to customary card-and-signature safe-deposit box access.

are learned or acquired. Biometrics actually serve a dual purpose—first, confirming a *positive identification* or proving that an individual is who he/she says he/she is and secondly, confirming a *negative identification*, or proving that he/she is not who he/she says he/she is.

Biometrics can be used in a very practical way in our everyday lives. In a *positive identification* scenario, an individual submits a “live” sample, such as a fingerprint, to a biometrics

number of financial institutions. The following are some of the more widely used biometric solutions.

Fingerprinting. Fingerprint scanning is the most widely used biometric application today, accounting for about 50 percent of the overall market. This is due in large part to its reliability and cost effectiveness. Fingerprint readers and scanners are used by some of the largest financial institutions for IT

more secure alternative to customary card-and-signature safe-deposit box access. Depository institutions may also realize security-related benefits in the areas of online transactions and employee computer access. Fingerprinting has also been the subject of significant research over the past several decades, increasing its public visibility. Finally, fingerprint sampling units are accurate, sturdy, compact, and less susceptible to forgery.

Voice Recognition. Voice recognition technology remains a second-tier alternative among current biometric alternatives. Difficulties arise with

³ See the Biometric Consortium’s *An Introduction to Biometrics* at <www.biometrics.org/html/introduction.html>.

⁴ See the Electronic Frontier Foundation’s *Who’s Watching You* at <www.eff.org/Privacy/Surveillance/biometrics/>.

⁵ *Ibid.*

continued on page 10

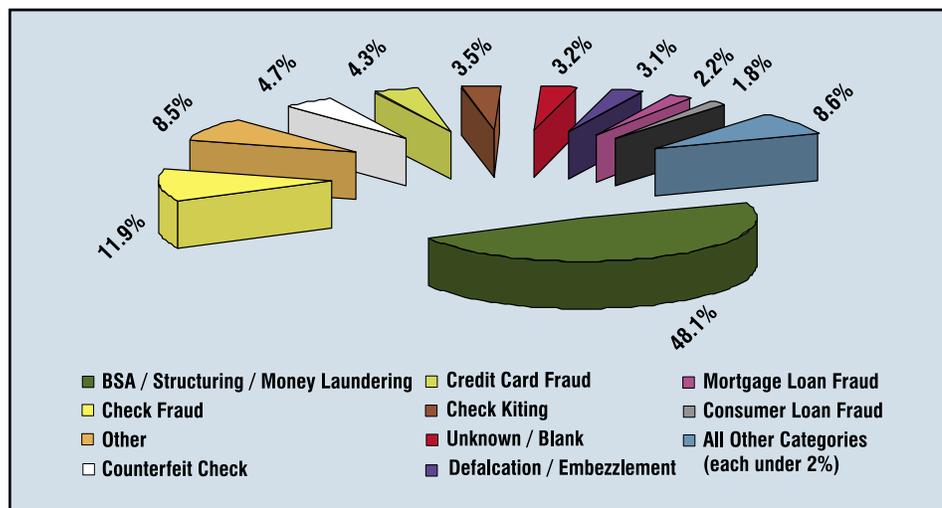
“Suspicious Activity Report (SAR) Filings” continued from page 3

representing 24.1 percent of all filings, followed by New York with 11.7 percent, and Florida and Texas with 6.3 percent each. Due to the size and geographic location of these states, this is probably not surprising. What is more surprising is that New Jersey ranks seventh with 2.8 percent,

Structuring/Money Laundering is the most common category, representing 48.1 percent of all filings from April 1996 through December 2003. Check Fraud, Check Kiting, and Counterfeit Checks collectively represent the second largest grouping, totaling 20.1 percent during this period.

trends and profile are vastly different from the national trend and profile. This is understandable considering the profile of institutions headquartered in Delaware and their emphasis on credit card lending, which explains the significantly higher proportion of SARs filed for Check Fraud and Credit Card Fraud. New Jersey and Pennsylvania’s reporting trends and profile more closely represent the national trend with only slight deviations.

Exhibit 2.
Top Ten SAR Violations Types For the Nation (4/96 - 12/03)



Pennsylvania ranks eighth with 2.5 percent, and Delaware ranks eleventh with 2.2 percent. Collectively, the top ten states represent over 65 percent of all SAR filings.

Many factors contributed to the significant increase in SAR filings, but most are related to the events of September 11. An increased awareness by financial institutions coupled with the expanded filing requirements in the USA PATRIOT Act have both contributed to the increase.

The Reasons. There are currently 22 violation categories under which SARs can be filed, but BSA/

Reflecting the changing environment, Computer Intrusion was added as a new category in June 2000, and the number of filings quickly grew from 419 in 2001 to 4,713 in 2003 (included in “Other” in Exhibit 2). In July 2003, Identity Theft and Terrorist Financing were added as new categories and 3,165 SARs were filed during the first five months for Identity Theft and 495 were filed for Terrorist Financing (both included in “Other” in Exhibit 2).

Table 1 summarizes the violations cited in SARs filed in the three states comprising the Third District and in the nation. Delaware’s reporting

The Consequences. For the SAR program to be effective, the information reported has to be accurate and complete. In a review of approximately 300,000 SARs filed between July 1, 2002 and June 30, 2003,³ FinCEN found that:

- Four percent were filed without a suspect name.
- Eight percent did not list an address for the suspect.
- Twenty-three percent did not provide the suspect’s social security number.
- Four percent did not provide any indication of what suspicious activity occurred.
- Six percent did not include a completed narrative.

³ See FinCEN’s *The SAR Activity Review Issue 6*, November 2003 at <www.fincen.gov/sarreviewissue6.pdf>.

Table 1. Analysis of 2003 SAR Filings*

	Delaware		New Jersey		Pennsylvania		U.S.	
	# of Filings	% of Filings	# of Filings	% of Filings	# of Filings	% of Filings	# of Filings	% of Filings
BSA/Structuring/ Money Laundering	478	5.19	6,525	57.09	4,093	50.16	155,468	48.54
Bribery/Gratuity	1	0.01	12	0.11	4	0.05	501	0.16
Check Fraud	1,035	11.24	1,322	11.57	1,239	15.19	35,740	11.16
Check Kiting	1,515	16.45	406	3.55	270	3.31	11,275	3.52
Commercial Loan Fraud	7	0.08	139	1.22	51	0.63	1,785	0.56
Computer Intrusion	5	0.05	14	0.12	14	0.17	4,713	1.47
Consumer Loan Fraud	344	3.73	68	0.59	86	1.05	4,536	1.42
Counterfeit Check	513	5.57	524	4.58	585	7.17	14,596	4.56
Counterfeit Credit/ Debit Card	62	0.67	11	0.10	20	0.25	1,392	0.43
Counterfeit Instrument (Other)	18	0.20	114	1.00	20	0.25	1,268	0.40
Credit Card Fraud	2,414	26.20	213	1.86	97	1.19	15,601	4.87
Debit Card Fraud	14	0.15	33	0.29	60	0.74	7,063	2.21
Defalcation/ Embezzlement	29	0.31	182	1.59	216	2.65	5,844	1.82
False Statement	163	1.77	182	1.59	137	1.68	4,978	1.55
Misuse of Position or Self Dealing	31	0.34	106	0.93	85	1.04	3,225	1.01
Mortgage Loan Fraud	11	0.12	141	1.23	248	3.04	9,539	2.98
Mysterious Disappearance	4	0.04	119	1.04	147	1.80	2,577	0.80
Wire Transfer	491	5.33	122	1.07	75	0.92	6,660	2.08
Terrorist Financing	4	0.04	22	0.19	13	0.16	495	0.15
Identity Theft	438	4.75	25	0.22	39	0.48	3,165	0.99
Other	1,635	17.76	1,150	10.06	660	8.09	29,835	9.32
Total	9,212		11,430		8,159		320,256	

* Since multiple violations can be reported on each SAR, the number of violations exceeds the number of SAR filings.

Accurate and complete information is not only essential for law enforcement to do their job, but it also saves time by reducing the need for follow up calls to the financial institution.

The Secretary of the Treasury has delegated primary responsibility for criminal enforcement of the BSA as it pertains to financial institutions to FinCEN, and failure to file accurate or

complete SARs can subject a financial institution to paying significant civil money penalties. Recent examples include the following.⁴

⁴ A complete list of FinCEN enforcement actions is available on its web site at <www.fincen.gov/reg_enforcement.html>.

- In 2002, Great Eastern Bank of Florida in Miami, Florida was subject to a \$100 thousand fine for failure to file SARs and failure to file complete SARs.
- In 2003, Banco Popular de Puerto Rico was assessed a \$20 million penalty for violations of the BSA. The press release stated that, "Although

the bank filed SARs on these accounts, they were untimely or, in some cases, inaccurate.”

- In 2004, the Office of the Comptroller of the Currency (OCC) and FinCEN concurrently fined Riggs Bank in Washington, D.C. \$25 million for, in part, failure to file approximately 33 SARs on a timely basis.

It is clear and imperative that financial institutions not only file complete and sufficient SARs but that the SARs are filed within the established timeframes. FinCEN has issued guidance on completing an accurate SAR in its *Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative*.⁵ Questions related to Suspicious Activity Reporting can also be referred to the FinCEN Regulatory Help Line at (800) 949-2732.

Final Thoughts

Although the SAR reporting program has existed for a number of years, it has recently received additional focus by Congress and bank regulators due to the highly publicized weaknesses found at Riggs Bank. In addition, over the past few years, compliance and operational risk have become of much greater importance to the financial industry, stemming from highly publicized failures in corporate governance.

Compliance and operational controls are not just areas that auditors and regulators force management to ad-

⁵ *Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative* is available on FinCEN's web site at www.fincen.gov/sarnarrcompleguidfinal_112003.pdf.

dress. In today's environment, both are essential ingredients in ensuring an institution can operate profitably, serve its community, and maintain its reputation, while minimizing its operational and legal risks. Improved risk management practices, such as the strong emphasis on Enterprise-wide Risk Management (ERM), have also helped to focus business leaders on compliance and operational risks.

If you have any questions on the filing of SARs, please contact your primary banking regulator. If you are supervised by the Federal Reserve Bank of Philadelphia, please contact your institution's central point of contact or assigned manager at the Reserve Bank. You may also contact Frank J. Doto (frank.doto@phil.frb.org) at (215) 574-4304 or William J. Brown (william.j.brown@phil.frb.org) at (215) 574-7291. ■

New Exam Procedures for Section 326 of USA PATRIOT Act

On July 28, 2004, the federal financial institution regulatory agencies issued procedures for examining domestic and foreign banking organizations' customer identification programs (CIP). The need for each institution to have a CIP was discussed in the article "Know Your Customer: It's Not Just a Good Idea, It's the Law!" that appeared in the second quarter 2004 issue of *SRC Insights*. The new examination procedures are designed to help financial institutions fully implement the new CIP requirements and facilitate a consistent supervisory approach among the federal financial institution regulatory agencies.

"Know Your Customer: It's Not Just a Good Idea, It's the Law!" is available on the Federal Reserve Bank of Philadelphia's web site at www.phil.frb.org/src/srcinsights/srcinsights/q2si4_04.html.

The new examination procedures are available on the Board of Governors' web site at www.federalreserve.gov/boarddocs/press/bcreg/2004/20040728/default.htm.

COVER STORY

“The Changing Supervisory Landscape”

continued from page 1

state and federal charters. At year-end 1984, there were 17,914 banking and thrift organizations nationwide, with 504 headquartered in the Third Federal Reserve District. By year-end 2003, those numbers had fallen to 9,182 and 287, respectively, declines of 49 percent and 43 percent. During the same period, 3,457 new banking organizations were formed, 158 of which were in the Third District.

While consolidation in charters continues, albeit at a slower pace, the number of branches continues to increase, reaching almost 80,000 in 2003, compared to 62,319 in 1984. Drivers of this changing distribution channel include customers' preferences for branch locations, in addition to electronic access and the ability of banks to manage branch offices profitably, offsetting higher operating expenses with noninterest income.

During this period of bank consolidation, industry assets increased 150 percent to \$9.1 trillion, and business models became more complex and diversified. However, this diversification did help the industry weather the latest economic downturn better than those in the past.

What have these changes meant for bank supervisors? Federal and state supervisors remain focused on ensuring the safety and soundness of financial institutions, ensuring stability in the financial markets, and ensuring fair and equitable treatment of consumers. In addition, as these organizations have become more complex and more

diversified, traditional supervision is complemented by private sector parties engaged in counterparty supervision.

However, the increasing complexity of the banking business means that factors other than traditional asset quality and interest rate risk con-

cerns can cause significant problems. Accordingly, we as supervisors have adapted our practices in response to increased financial institution emphasis on more sophisticated risk management and measurement processes. Financial modernization, evolution of the Federal Reserve System's role as consolidated (umbrella) supervisor, increasingly active functional regulators and law enforcement agencies, and the proposed Basel Capital Accord (Basel II) have all shaped our supervisory processes. In addition, in response to the segmentation of the industry into a large, complex banking organization segment, a regional banking segment, and a community banking segment, and reflecting community bank managements' concerns about supervisory burden, we continue to focus on customizing and streamlining community bank examination processes.

These structural changes, the low interest rate environment, and the renewed emphasis on fee income have created additional interest in subprime lending and fringe banking products. A subset of subprime lending, predatory lending, and a related activity, payday lending,

The increasing complexity of the banking business means that factors other than traditional asset quality and interest rate risk concerns can cause significant problems.

have increased compliance risk at participating institutions. To better ensure a successful franchise, bank management should gain a deeper understanding of how risks develop, manage conflicts of interest across business lines, and make sound strategic decisions about the risk/reward value proposition of new and current products, services, and delivery channels.

The Federal Reserve must maintain a meaningful role in supervision to promote financial stability, contribute to sound public policies, and complement its other central bank responsibilities. The ability to recruit, develop, retain, and deploy staff with the skills and expertise to understand and assess risks will allow the System to remain a premier bank supervisor and conduct value-added supervision at the institutions that it supervises. ■

“Biometrics: A Viable Solution?”

continued from page 5

the voice compression associated with microphones and handsets, background noise, and changes in the human voice as a result of aging, stress, and fatigue. This presents difficulties for computers in the positive identification of individuals. However, voice recognition does allow for remote identification using existing phone lines, which would eliminate much of the up-front costs associated with normal biometric identification program startups.

Signature Verification. Signature verification is the process used to distinguish an individual's handwritten signature. To confirm the identity of a user during the verification process, changes in the speed, shape, and pressure of an individual's signature are measured. A rudimentary form of this verification process is typically used today by depository institutions when bank tellers verify the signature of an account holder making a transaction. The consistency of a signature is most important, since ordinary motions and patterns will assist in the creation of a recognizable pattern for biometric identification.

Iris/Retina Scanning. Originally proposed by ophthalmologist Frank Burch in 1936, iris/retina scanning analyzes the unique features of the colored tissue surrounding the pupil, which includes corona, filaments, striations, and other identifiers. Iris scanning provides a very attractive and accurate alternative for authentication, identification, and verification. However, start-up costs remain extremely high, and issues of

operational difficulty and training remain.

Facial Recognition. First introduced in the late 1980s, facial recognition analyzes the characteristics of an individual subject's face image, including overall facial structure and spatial measurements between the nose, eyes, jaw, and mouth. Measurements are retained in a database and are used for comparison when an individual stands before a camera. This technology is gaining support in the anti-terrorist community because of its apparent non-intrusive nature. Concerns have been raised, however, over the use of facial recognition technology because of its perceived infringement upon an individual's right to privacy, especially if used in public places such as airports, restaurants, and sporting facilities.

Hand Geometry. Employed at nearly 8,000 locations worldwide, hand geometry involves the measurement and analysis of the shape of an individual's hand. Unlike fingerprints, hand features are not unique; however, using a combination of independent variables, verification can be achieved. Hand geometry is easy to use, requires very little data, and is virtually impossible to manipulate. The difficulty associated with this technology rests in its accuracy, cost, device size, and possible user problems as a result of physical changes to hand geometry.

Selected Legislative and Regulatory Action

A number of legislative and regulatory initiatives have been adopted over the

past several years that incorporate biometric solutions as key components of an overall strategy to improve national security and reduce fraud. The following are some of the significant initiatives in these areas:

- The **USA PATRIOT Act** requires the federal government to develop and certify a technology standard that can be used to verify persons applying for or seeking entry into the United States on a visa. The *Enhanced Border Security and Visa Entry Reform Act of 2002* requires that only machine readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers be issued to aliens after October 26, 2004.
- The **Fair and Accurate Credit Transactions Act of 2003 (FACT)**, signed by President Bush on December 4, 2003, made significant changes to the *Fair Credit Reporting Act (FCRA)*, which will provide consumers, companies, credit reporting agencies, and regulators with new tools in the fight against identity theft. The FACT Act provides for a free annual credit report, allows for the receipt of a credit score from a credit reporting agency, increases the standard for accuracy in credit reports, reinforces the need for adverse action notices, and creates a national fraud detection system to protect consumers against identity theft. The Act also requires federal regulators such as the Treasury Department to study how biometrics

can help prevent identity theft and to solicit public comments regarding the costs, risks, and uses of biometric technologies. The Treasury Department released a 14-point survey in the March 2, 2004 *Federal Register* to comply with this requirement.^{6,7} Responses from individual entities and the general public were due on April 1, 2004, with a report to Congress required in June 2004.

- The *Department of Homeland Security* has been a strong advocate of biometric solutions to curtail unauthorized entry in the United States. The U.S. Attorney General and the Secretary of State have been directed by Congress to issue to aliens only visas and other travel and entry documents that use biometric technologies. Each country certified to participate in the visa waiver program has been instructed to certify that it has a program to issue to its nationals passports that incorporate biometric authentication identifiers. Both the Transportation Security Administration and the Immigration and Naturalization Service have released policies, which conform with the Department of Homeland Security policies concerning the use of biometric technologies for foreign travelers.

- The *Federal Financial Institutions Examination Council* (FFIEC) is an interagency body of federal financial institution regulators responsible for establishing uniform principles, standards, and report forms. On August 8, 2001, the FFIEC released guidance, which focused on the inherent risks and risk management practices related to authentication in the electronic banking environ-

Federal Reserve SR Letter 03-10
The Federal Reserve System and the Federal Bureau of Investigation (FBI) have enhanced the Federal Reserve System's name check requirements under the *Bank Holding Company Act* and *Change in Bank Control Act*. Under these Acts, individuals who would "control" an insured depository institution must first secure regulatory approval. As part of this approval process, the Federal Reserve usually

Biometrics contain unique authentication advantages, which may be beneficial to financial institutions.

ment, and provided considerations for the implementation and use of biometric technologies by financial institutions. The FFIEC also set forth administrative and logistical standards for secure biometric systems in its *Information Security Booklet*.⁸ According to the FFIEC, biometrics contain unique authentication advantages, which may be beneficial to financial institutions. The booklet addresses issues related to biometric technologies associated with the recording of physical characteristics, establishment of secure enrollment devices, and acceptable probability and statistical confidence levels.

conducts name checks on individuals associated with the proposed transaction.

In SR Letter 03-10, *Enhancement to the Name Check Process Related to Applications Reviewed by the Federal Reserve*, released on May 28, 2003, fingerprinting has been added to supplement the overall criminal history and name check process. The Federal Reserve uses two methods to obtain fingerprints—LiveScan terminals and fingerprint cards. Currently, eight Federal Reserve banks, including Philadelphia, use LiveScan terminals. Important guidance related to the applicability of SR 03-10 can be found in the instructions to the *Interagency Biographical and Financial Report*, Form FR 2081(c).⁹ Applications or notices received after June 30, 2003, are subject to the new fingerprinting procedure.¹⁰

The Evolving Market for Biometric Technologies

Growth in the biometrics market is expected to be driven by the global

⁶ *American Banker*, Fact Act Provision Raises Biometrics' Profile, March 17, 2004.

⁷ The *Federal Register* notice is available at <a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2004/pdf/04-4604.pdf>.

⁸ The *Information Security Booklet* is available on FFIEC's web site at <www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec>.

focus on security. Global biometric revenues generated during 2001 totaled \$524 million, with 65 percent of that from law enforcement and the public sector. In the United States, the \$10 billion US-VISIT (Visitor and Immigrant Status Indicator Technology) Program was piloted in November 2003 by the Department of Homeland Security. This program is designed to collect and retain biographic, travel, and biometric information about visitors to the U.S. Nationwide implementation of the security program occurred on January 5, 2004 at 115 U.S. airports and in cruise ship terminals at 14 U.S. seaports.

On April 26, 2004, Great Britain announced plans to introduce identity cards to stem illegal immigration and defend against possible terrorist attacks. Pilot trials for the new identity program began in April 2004 and have included 10,000 volunteers nationwide.¹¹ An integral part of the new identity card program will be the use of a national database containing the facial dimensions, iris images, and fingerprints of individuals. According to Great Britain's Home Security Office, biometric data will be used for passports and driving licenses before compulsory identification cards are

eventually rolled-out sometime in 2013.

Financial institutions currently reviewing the feasibility of biometric systems include the following:

- **Associated Bank** - implemented voiceprint technology in June 2003. The technology is designed to improve security for the Bank's e-business initiatives by increasing the "probability" of identifying online users.¹²
- **Fidelity Investments** - pilot testing a voice recognition system to authenticate customers conducting telephone transactions.¹³
- **Bank of America** - testing fingerprint ID for customers.¹⁴
- **United Banker's Bank** - using fingerprint technology for customers and employees.¹⁵
- **American Express** - using fingerprint biometrics for physical access.¹⁶
- **Mellon Bank** - using fingerprint biometrics for background checks.¹⁷
- **California Commerce Bank** - using fingerprint biometrics for network access.¹⁸

- **InTrust Bank** - using voice recognition for bank transactions.¹⁹
- **Western Bank** - using signature-based biometrics for financial transactions.²⁰
- **First American Bank** - using signature-based biometrics for document processing.²¹
- **First Tennessee Bank** - using signature/hand biometrics for vault access.²²
- **Bank of Hawaii** - using signature/hand biometrics for vault access.²³
- **Zion First National Bank** - using signature/hand biometrics for vault access.²⁴

Although the global market for biometric solutions has experienced measurable growth, the United States market still remains the catalyst for global acceptance. The global market has not expanded as rapidly as most industry analysts would have predicted, due primarily to a downturn in the world economy and United States' foreign policy issues which have delayed finalization of private and public sector contracts. These concerns notwithstanding, it would seem that the delay in adoption of biometric solutions is more a matter of timing than of product legitimacy, since many of the delayed projects remain under consideration by clients.

Considerations for Financial Institutions

As with any emerging technology, biometric solutions present unique challenges. Some issues related to biometrics will dissolve naturally,

¹² The Business Journal, *Associated Bank Adopts Voice Print*, April 25, 2003, at <milwaukee.bizjournals.com/milwaukee/stories/2003/04/28/story5.html>.

¹³ Info World, *Fidelity Looks to Biometrics to ID Clients, Employees*, April 8, 2003.

¹⁴ Computer Weekly.com, *Bank Tests Bluetooth-based Biometric ID System*, May 12, 2004, at <www.computerweekly.com/articles/article.asp?liArticleID=130506&liArticleTypeID=1&liCategoryID=1&liChannelID=7&liFlavourID=1&sSearch=&nPage=1>.

¹⁵ Security, *Banking on Biometrics*, April 10, 2004, at <www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,123069,00.html>.

¹⁶⁻²⁴ Digital ID World.com, *Biometrics and Financial Services - Show Me the Money!*, January/February 2004, at <magazine.digitalidworld.com/Jan04/Page20.pdf>.

⁹ The *Interagency Biographical and Financial Report* is available on the Board of Governors web site at <www.federalreserve.gov/boarddocs/reportforms/formsFR_2081c20030328_f.pdf>.

¹⁰ For additional information regarding SR Letter 03-10, see James D. DePowell's article "New to Banking? Fingerprints May be Required" in the Third Quarter 2003 issue of *SRC Insights* at <www.phil.frb.org/src/srcinsights/srcinsights/q3si4_03.cfm>.

¹¹ Reuters, *Britain Faces Prospect of High Tech ID Cards*, April 26, 2004.

while others will require more targeted approaches. There are a number of issues financial institutions should consider before making an investment in a particular biometric solution. First, in general, biometric solutions still remain a cost prohibitive alternative for many small to medium-sized financial institutions. Although prices are expected to fall, fingerprinting devices and iris scanning devices sell for around \$100 and \$300 per unit, respectively, while face recognition systems start at \$15,000 per unit. The maintenance of these systems also presents a cost concern, since hardware to capture biometrics and the databases and servers that house and process the information remain expensive.

Beyond price, user education can be lengthy and sometimes cumbersome, and gaining acceptance of biometric applications by both employees and customers may be problematic. Other concerns related to the use of biometrics by financial institutions may include:

- The time constraints associated with the development of a realistic threat model that identifies targets and the threats they pose.
- The quality of risk data used.
- The reliability of information collected through the initial enrollment or registration process.
- The implementation of a solution that exceeds an institution's security and authentication needs.
- Concerns about the discriminatory and dehumanizing aspects of collecting, storing, and using biometric information.

- The storage of central templates.
- The need for extensive testing prior to deployment.

The Future of Biometrics

The financial services industry has traditionally been difficult for biometrics solutions to penetrate, due in large part to the cost prohibitive nature of the technology and consumer concerns regarding privacy and convenience. Cultural, political, and legal issues associated with biometrics continue to confront financial institutions, while issues of size, convenience, speed, accuracy,

take place? Much of the focus post-September 11 has been on security issues and the government's desire for public safety in transportation, immigration, and border management. However, for the biometrics industry to survive and flourish, future efforts must focus on providing viable solutions for financial institutions, keeping in mind concerns about privacy and civil liberties. Encouraging signs have begun to emerge that show biometrics have become part of the lexicon of financial institutions. Serious discussions are taking place at all levels of government and in corporate boardrooms regarding the

Serious discussions are taking place at all levels of government and in corporate boardrooms regarding the role of biometrics in the areas of physical security, data management, and data storage.

connectivity, and compatibility remain largely unanswered. Biometric vendors have attempted to address these concerns by offering more affordable, accurate, and compatible devices that can be easily installed and configured to meet the unique needs of financial institutions. Also helping biometrics win acceptance has been legislative, regulatory, and public recognition. There has also been encouraging work by the U.S. Biometric Consortium and the International Biometric Group in the development of uniform measurements, standards, and testing.

Where will the opportunities for biometric technology occur, so that sustainable, quantifiable growth can

role of biometrics in the areas of physical security, data management, and data storage. As capital spending becomes more elastic, privacy concerns are addressed, uniform standards are adopted, and geo-political issues are resolved, we are likely to see biometric solutions play a more integral role in the overall operations of financial institutions well into the future.

If you have any questions regarding this article, please contact Frederick W. Stakelbeck, Jr., Training and Development Coordinator, (frederick.w.stakelbeck@phil.frb.org) at (215) 574-6422. ■

From BOPEC to RFI: A Change is Coming

In 1979, the Federal Reserve System implemented a bank holding company (BHC) rating system to define the condition of a BHC in a systemic and consistent manner. This system—known as BOPEC/F–M for the components that it rated—served three purposes: (i) providing a summary evaluation of the BHC’s condition for use by the supervisory community; (ii) forming the basis of supervisory responses and actions; and (iii) providing the basis for supervisors’ discussions with BHC management.

rating the potential impact of non-depository subsidiaries of a BHC on the subsidiary depository institutions. Accordingly, although there would be only five component and composite ratings—RFI/C (D)—they would be supported by eight subcomponents. With the exception of the four risk management subcomponents, which would be rated Strong, Adequate, or Weak, the composite, components, and subcomponents would continue to be rated on a 1 to 5 numeric scale, with a 1 indicating the highest rating.

Consistent with the System's risk-focused approaches to bank and BHC supervision, not all BHCs would be subject to the new rating system. Noncomplex BHCs with assets of \$1 billion or less—essentially shell BHCs—would be assigned only an R and C rating. All other BHCs would receive the full RFI/C (D) rating, but the degree of emphasis on each of the components would vary based on each institution’s circumstances.

A complete discussion of the proposal and an invitation to comment is available in the *Federal Register* or on the Board of Governor’s web site.² Comments are due to the Board by September 21, 2004. ■

Today: BOPEC/F–M

- B = Condition of banking subsidiary(ies)
- O = Condition of nonbank subsidiary(ies)
- P = Condition of parent company
- E = Consolidated earnings position of BHC
- C = Consolidated capital position of BHC
- F = Financial composite rating
- M = Management composite rating

On July 23, 2004, the Federal Reserve published in the *Federal Register* a notice and request for comment on a proposed revised BHC rating system.¹ The new rating system would emphasize risk management, provide a more comprehensive framework for assessing financial factors, and provide a framework for assessing and

¹ The notice and request for comment is available in the *Federal Register* at <a257.g.akamaitech.net/7/257/2422/06jun20041800/edocket.access.gpo.gov/2004/pdf/04-16865.pdf>.

² The notice and request for comment is also available on the Board of Governors’ web site at <www.federalreserve.gov/boarddocs/press/bcreg/2004/20040723/default.htm>.

... and Tomorrow?: RFI/C (D)

- R = Risk management
 - Competence of Board and Senior Management
 - Policies, Procedures, and Limits
 - Risk Monitoring and Management Information Systems
 - Internal Controls
- F = Financial condition
 - Capital
 - Asset Quality
 - Earnings
 - Liquidity
- I = Impact of parent company and nondepository entities on subsidiary depository institutions
- C = Composite rating
- (D) = Generally mirrors the primary regulator’s assessment of subsidiary depository institutions

Whom To Call?

Financial institution management may need to contact an officer, manager, or staff in the Supervision, Regulation & Credit Department but not know whom to call. The following list should help management identify to whom to raise their questions. Financial institutions that have an appointed central point of contact should generally contact that individual directly.

Contact names appearing in **bold** are the primary contacts for their areas.

Community, Regional, and Global Supervision

John J. Deibel, VP 574-4141
Elisabeth V. Levins, AVP 574-3438
Douglas A. Skinner, Manager 574-4310
William T. Wisser, Manager 574-7267

Eric A. Sonnheim, AVP 574-4116
John V. Mendell, Manager 574-4139
Glenn A. Fuir, Manager 574-7286

Capital Markets

John J. Deibel, VP 574-4141
Elisabeth V. Levins, AVP 574-3438
Avi Peled, Manager 574-6268

Consumer Compliance & CRA Examinations

John J. Deibel, VP 574-4141
Constance H. Wallgren, AVP 574-6217
Robin P. Myers, Manager 574-4182

Consumer Complaints

John J. Deibel, VP 574-4141
Constance H. Wallgren, AVP 574-6217
John D. Fields 574-6044
Denise E. Mosley 574-3729

Regulations Assistance

Regulations Assistance Line 574-6568

Enforcement

A. Reed Raymond, VP 574-6483
William L. Gaunt, AVP 574-6167
Frank J. Doto, Enforcement
and Surveillance Officer 574-4304

Regulatory Applications

A. Reed Raymond, VP 574-6483
William L. Gaunt, AVP 574-6167
James D. DePowell, Manager 574-4153

Retail Risk Analysis

William W. Lang, VP 574-7225
Todd Vermilyea, Manager 574-4125

Discount Window and Reserve Analysis

Vish P. Viswanathan, VP 574-6403
Gail L. Todd, Manager 574-3886



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. 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.

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.phil.frb.org/phil_mailing_list/dsp_user_login.cfm.