



Insights

FEDERAL RESERVE BANK OF PHILADELPHIA

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

Volume 6 Issue 3

IN THIS ISSUE

SVP Commentary 1

A New Age of Anti-Money Laundering 2

A Message From Lou Sanfelice 2

Fraud Prevention: Risk Mitigation Principles and Techniques for Payment Card Operations 4

Compliance Corner CC1

CIRCULATE TO:

- _____
- _____
- _____
- _____

SVP Commentary on...

The Human Aspects of Contingency Planning

by Michael E. Collins

Many businesses gained significant benefits from the development of Year 2000 contingency and event management plans. During the years leading up to January 1, 2000, contingency planning evolved from a largely theoretical exercise to a problem solving and training tool that could help organizations respond promptly to operational failures and natural disasters. Companies developed more detailed contingency plans by analyzing the effect of potential system failures on core business processes; determining the minimum acceptable level of output and services for each core business process; testing the contingency plans; and validating the results through independent parties. They also recognized the need to review and plan for contingencies related to all aspects of the company's operating environment, including IT systems and non-IT systems.

Since the primary perceived weakness – the lack of century coding on computers – was technological, the focus of Year 2000 contingency planning was on “systems.” This systems



continued on page 6

A New Age of Anti-Money Laundering

by Daniel L. Hutchinson, Supervising Examiner

In the aftermath of the horrific events of September 11, President Bush and the Congress have reacted decisively on varied fronts to meet the continuing threats posed by international terrorists. Recognizing that unfettered access to the global payments system allows terrorists to pay and receive funds in support of their operations, the United States and many other concerned countries are in the process of strengthening and expanding existing tools to more effectively monitor and interdict funds transfers related to terrorism. This article will discuss some of the actions being taken and their implications for banks operating in the U.S. and abroad. The comments are descriptive only and do not purport to interpret law. Interested parties are encouraged to access the source references.

An important action taken by Congress, which was signed into law on October 26, 2001 by the President, was the passage of Title III of H.R. 3162, the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001*.¹ This law was in the making for some time prior to September 11, so it had been given considerable scrutiny and was not devised hurriedly. It reflects nearly 25 years of experience with successes and failures in the fight against criminal use of the banking system.

It builds on an existing framework of laws, regulations, policies, and procedures that are well known and that have resulted in some important setbacks to narcotics dealers and other criminal elements. The nature of terrorist operations is sufficiently different from the more familiar drug schemes that new and broader powers have been given to law enforcement agencies, regulators, and banking institutions to deter and detect criminal financial activity relating to terrorism. Some of these powers are granted in new law, but most are reflected in amendments to existing law.

Anti-Money Laundering Provisions

Not the least important amendment is the strengthening of so-called “safe-harbor” protection extended to financial institutions, their officers, directors, and employees who voluntarily divulge to authorities information about financial transactions that would ordinarily be considered privileged. This amendment expands existing immunity from liability for making such disclosures. Other amendments require each financial institution to establish anti-money laundering programs that, at a minimum, address internal policies, procedures, and controls for anti-money laundering programs; designate a compliance officer; provide for an on-going employee training program; and provide for independent audits to test the programs. Other amendments require registered securities brokers and dealers to file suspicious activity reports; grant access by U.S. intelligence agencies to records of account information maintained by financial institutions; subject to suspicious activity reporting (SAR) requirements any person engaged in the transmission of funds outside of the conventional financial institutions system; and, to support the increased level of surveillance, upgrade the Financial Crimes Enforcement Network (FinCEN)² to Bureau status within the Treasury Department with a special hot line for reporting suspicious activities

A Message From Lou Sanfelice

As some of you may know, I retired from the Federal Reserve on February 1, 2002. During my years with the Fed, I witnessed many changes in the banking industry and was very fortunate to have had many opportunities to meet with Third District bankers, directors, other regulators, and industry groups.

I have many wonderful memories and, of course, wish each of you success and good health.

¹ See the *USA Patriot Act of 2001* at <thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.enr>.

² See FinCEN’s web site at <www.treas.gov/fincen/>.

related to terrorism (1-866-556-3974).

Amendments also address the stated legislative intent, which was “to provide a clear national mandate for subjecting to special scrutiny those foreign jurisdictions, financial institutions operating outside of the United States, and classes of international transactions or types of accounts that pose particular, identifiable opportunities for criminal abuse” (i.e., “of primary money laundering concern”).³ Specifically identified are enhanced record keeping and reporting, more complete information relating to beneficial ownership of accounts owned by foreigners in the United States, and detailed information about payable through and correspondent accounts opened in the United States and owned by foreigners. Covered financial institutions are prohibited from establishing correspondent accounts with foreign shell banks (i.e., a foreign bank that does not have a physical presence in any country).

Anti-Money Laundering Responsibilities

Banks are not destined to shoulder the entire anti-money laundering burden. The Treasury Department – essentially the lead U.S. Government agency for developing and implementing appropriate policies in consultation with relevant regulatory, judicial, and intelligence counterparts – has an ambitious national strategy for anti-money laundering

action both domestically and internationally. The Department’s goals as articulated in *The 2001 National Money Laundering Strategy* are:

- Focus law enforcement efforts on the prosecution of major money laundering organizations and systems
- Measure the effectiveness of anti-money laundering efforts

- Prevent money laundering through cooperative public-private efforts and necessary regulatory measures
- Coordinate law enforcement efforts with state and local governments to fight money laundering throughout the United States
- Strengthen international cooperation to combat the global problem of money laundering⁴

While banks play an essential role in the process, it is clear that many public and other private institutions are contributing resources to the anti-money laundering effort. The

banking privacy paradigm is shifting away from absolute privacy of individual relationships to a standard that speaks to the national security interest and international concerns about the abuse of the financial system for criminal and terrorism purposes. Today’s framework of legislation, institutions, and task forces has the formidable potential to severely inhibit, if not totally eradicate, money laundering. What is needed for success is the proactive participation of the key players,

The banking privacy paradigm is shifting away from absolute privacy of individual relationships.

domestic and international, public and private.

Know Your Customer

The Federal Reserve and other regulatory agencies have long been active in setting standards for bank compliance with the developing body of anti-money laundering regulations. Experience tells us that one of the thorniest compliance areas is the “know your customer” requirements. Relationship managers and senior bank officials are reluctant to be perceived by customers or prospects as intrusively inquisitive about the sources and extent of bankable assets. Yet, such knowledge is the most essential element underlying a financial institution’s ability to gauge the appropriateness of transactions

continued on page 8

³ See §302(b)(4) of the *USA Patriot Act* at <thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.enr:>.

⁴ See *The 2001 National Money Laundering Strategy* at <www.treas.gov/press/releases/docs/ml2001.pdf>.

Fraud Prevention: Risk Mitigation Principles and Techniques for Payment Card Operations

by Frederick W. Stakelbeck, Jr., *Payment Cards Analyst*

The Fraud Prevention Department is a central component within a card issuing operational infrastructure. In coordination with other departments – such as audit, collections, credit policy, customer service, and marketing – the Fraud Prevention Department provides a specialized service for the interdiction of fraud. How it accomplishes its mission, the tools it uses, and its interaction with accountholders largely determine its success or effectiveness.

The central mission of the Fraud Prevention Department is the reduction of fraud losses associated with the use of payment cards (e.g., ATM, debit, and credit cards) through the preemptive identification and control of high-risk accounts. To achieve this risk-management mission, close interaction with internal investigators, law enforcement officials, and payment card associations is essential. In addition, fraud prevention must also utilize a myriad of tools – including account decisioning models, scalable software applications, and prevailing account management principles – to implement an organization's accountholder credit policy controls and monitor performance in accordance with cardholder agreements.

Organizational Structure and Staffing

The Fraud Prevention Department's operational structure should reflect the diversity of the payment card products offered, the scale of the issuer's portfolio, actual or perceived systemic

risk, and the issuer's commitment to sustained growth. Typically, the Chief Credit or Risk Management Officer heads the Fraud Prevention Department. The Department generally contains separate units for administrative support, credit risk management, fraud policy and analysis, investigations, and quality assurance. Staffing may include fraud prevention analysts, credit policy analysts, and administrative support.

Fraud prevention analysts are a select group of individuals who possess a mélange of expertise and knowledge in the behavioral sciences, credit risk management, finance, economics, and law. This combination of expertise and knowledge uniquely qualifies them to work with accountholder issues. Previous issuer experience in areas such as administration, customer service, collections, and investigations adds to their intrinsic value.

Fraud Identification Tools

The ability of criminals and criminal organizations to effectively infiltrate, decipher, and manipulate the risk management infrastructure of financial institutions has spurred the development of numerous real-time predictive software products. Although effective proprietary software products have been developed and are in use by both large and small issuers, vendor-sponsored products remain the dominant force in the fraud prevention software market.

Real-time predictive software uses

rules-based technology to track individual payment card transactions. These systems, which are designed to reduce the occurrence of false positives, generate a "fraud score" for each individual transaction using neural network technology that allows fraud professionals to build models of complex transaction patterns using large data sets.

The fraud score indicates the possibility that an account transaction is fraudulent. Scores range from zero, a low probability of fraud, to 999, a high probability of fraud. A fraud prevention analyst automatically places accounts that meet high-risk criteria (e.g. jewelry purchase with a fraud score of over 699) into queues for review.

An issuer considers a number of variables when constructing high-risk fraud rules. Some of the more common variables include:

- Prior spending patterns
- Type of activity or transaction
- Age of the account
- Amount of the transaction
- Geographic location
- Time of day transaction occurred

Qualitative and Quantitative Reporting

The success of a Fraud Prevention Department is directly related to its ability to identify and eliminate fraudulent activity. Consequently, its success can be measured using a combination of qualitative and quantita-

tive reports. Qualitative reports, such as inter-office alerts and memoranda, are ordinarily distributed by management to fraud prevention analysts to apprise them of existing fraud trends, possible fraud suspects, and changes in departmental policy and strategies. On the other hand, quantitative reports are used to analyze, monitor, and report on the financial performance of an issuer. To accomplish this task, these reports are designed to capture information such as the following:

of fraud perpetrated, and transaction volume, management can make informed decisions that directly influence the prioritization of departmental objectives and the allocation of resources.

Staff Training and Performance

Fraud prevention analysts typically participate in an extensive training regimen that emphasizes demonstrated knowledge of software functionality, issuer internal controls, industry rules and regulations, and ac-

taken, or the total number of fraud reports taken.

Investigating and Processing Fraud Alerts

In addition to the identification of individual transactions by predictive software, several variations of account transaction activity may stimulate a review by a fraud prevention analyst, including these examples:

- The issuer receives notification from a third party, usually Visa or

Training of fraud prevention analysts is an on-going, interactive development process.

- Total number of accountholder calls taken
- Total amount of fraud losses realized
- Total number of fraudulent accounts identified
- Total amount of credit saved as a result of the department's preventive measures
- Total number of accountholder calls taken by each fraud prevention analyst
- Frequency of various types of fraud
- Identification of high-risk zip codes or countries of origin
- Identification of high-risk transactions

curate coding and documentation of accounts. Training of fraud prevention analysts is an on-going, interactive development process that involves the use of simulated call scenarios and random telephone monitoring to maximize analyst performance.

Benchmarks are standards or points of reference used by an issuer to measure performance. Fraud prevention analysts may be required to meet or exceed required quotas or target numbers created by the Department. Benchmarks may fluctuate, contingent upon department attrition rates, the total number of accounts for which an issuer is responsible, or the availability of innovative software technologies. Analyst performance can be measured by the total number of accountholder calls taken per hour, the total number of accounts reviewed per hour, the total number of actions

MasterCard, indicating that specific account numbers may have been compromised. The Fraud Prevention Department automatically blocks accounts until the questionable activity can be verified with the accountholder. As a precaution, accounts of this nature are usually closed and a new account number is issued.

- As a result of an arrest or investigation, law enforcement officials discover compromised account numbers or other supplementary evidence supporting an assertion of fraud. A temporary block will be placed on an account until the accountholder can be notified. Again, as a precaution, ac-

continued on page 10

COVER STORY

“Contingency Planning” continued from page 1

orientation to contingency planning enabled the financial markets to quickly return to normal after the attacks of September 11. Many companies managed to avoid even bigger catastrophes because of the increased focus on contingency and disaster plans leading up to Year 2000.

However, the challenges on and after September 11 highlighted the importance of another aspect of contingency planning – the human element. Contingency planning is not just about buildings and computers and papers; it is also about people and information and knowledge.

Contingency planning professionals acknowledge that protecting the health and safety of people is the first priority during an emergency. Accordingly, evacuation planning, evacuation routing, assembly and shelter, and evacuation training should be and generally are included in every contingency plan. Equally important, but more difficult to acknowledge, is planning for events when people do not survive. In the past, human resources rarely made the list of high priority management concerns when a business was planning for a disaster. Acknowledging that a significant number of staff might be lost is difficult to face. However, the terrorist attacks of September 11 changed forever the definition of disaster and the ways in which businesses will be expected to respond. Businesses now have to prepare for that which may be unpreparable.

Safeguarding records and equipment is easy compared to the task of replacing human capital. To ensure the continuity of the business, so-called battlefield promotions are necessary, but are painful for the company and the individuals involved. Consider the emotional impact of the promotions of New York Fire Department personnel so soon after September 11. Hiring after

Organizational compassion is necessary not only in times of widespread disaster but also in times of personal crisis.

a disaster is likewise difficult because people are dealing with grief and anxiety in addition to business concerns. However, businesses must still fill critical openings to minimize further financial loss, without seeming disrespectful to those who died. Well considered management succession plans, not just for the CEO and senior executives but also for line officials and managers, provide the foundation for sound professional development programs as well as seamless transitions from disasters.

Managing surviving staff provides as many challenges as replacing staff who are lost. Immediate, effective, and accurate communication with staff and their families is critical, not just

in the moments after the disaster but for weeks and months thereafter. The January 2002 issue of the *Harvard Business Review* contained an excellent article on the importance of strong leadership in times of trauma.¹ The article, which is based on three years of research conducted jointly by the University of Michigan Business School and the University of British Columbia, discusses how a leader’s ability to enable a compassionate response throughout a company directly affects the organization’s ability to maintain high performance in difficult times. This characteristic – called organizational compassion – helps people heal and continue with their work when times are bad. Organizational compassion is necessary not only in times of widespread disaster but also in times of personal crisis.

The article describes four indicators of an organization’s capacity for compassion – the scope of compassionate response, the scale of the response, the speed of the response, and the specialization of the response. The **scope** of the response refers to the breadth of resources provided to people in need. This

¹ See Jane E. Dutton, Peter J. Frost, Monica C. Worline, Jacoba M. Lilius, and Jason M. Kanov, “Leading in Times of Trauma,” *Harvard Business Review* January 2002:55, or order online from Harvard Business School Publishing at <www.hbsp.harvard.edu/products/hbr/jan02/R0201D.html>.

might include money and other benefits; flexibility in work schedules; providing for physical needs, such as shelter; and providing for emotional needs, ranging from an open ear to formal trauma counseling. The **scale** of the response refers to the volume of resources, time, and attention made available to those who are suffering. The **speed** of the response refers to how quickly and how continuously the resources are directed to the need. The **specialization** of the response refers to the degree to which the response is customized to the

situation. Each individual is unique, and their needs in a crisis will likewise be unique. As with managing staff on a day-to-day basis, compassion is not a “one size fits all” process.

I have frequently said that perhaps the single most valuable asset of a financial institution is the trust of its customers. I would like to clarify that. While the trust of your customers is your most valuable *intangible* asset, your staff is your most valuable *tangible* asset. You should never lose sight of their worth, whether in day-to-day

operations or in planning for a disaster.

I encourage you to carefully consider the human aspects of contingency planning as you revise your plans over the coming weeks and months. Much will be written about the experiences of companies with operations and staff in the World Trade Centers, and I encourage you to adopt the best practices of these organizations to better prepare your organization and your staff for challenges that might lay ahead. ■

Whom To Call?

Community, Regional, & Global Supervision

John J. Deibel, VP 574-4141
 Dianne Lee Houck 574-4138
 Elisabeth C. Videira-Dzeng, AVP ... 574-3438
 Bernard M. Wennemer, AVP 574-6485
 John V. Mendell 574-4139
 Douglas A. Skinner 574-4310
 Michael P. Zamulinsky, AVP 574-4136
 Robert E. Richardson 574-4135

Enforcement, Banking Surveillance, & Off-Site Integration

John J. Deibel, VP 574-4141
 Eileen P. Adezio, AVP 574-6045
 Mary G. Sacchetti 574-3848
 Frank J. Doto 574-4304

Payment Card Studies

John J. Deibel, VP 574-4141
 Glenn A. Fuir 574-7286

Consumer Compliance & CRA Supervision Consumer Complaints

A. Reed Raymond, VP 574-6483
 Constance H. Wallgren 574-6217

Regulatory Applications

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

Capital Markets & Special Studies

Joanna H. Frodin, VP 574-6419
 Avi Peled 574-6268
 Vincent J. Poppa 574-6492

Discount Window & Reserve Analysis

Vish P. Viswanathan, VP 574-6403
 Dennis S. Chapman 574-6596
 Gail L. Todd 574-3886

“A New Age” continued from page 3

conducted by or on behalf of its customers, and to determine whether a SAR should be filed. The importance of “know your customer” policies extends beyond individual or private banking relationships. The *USA Patriot Act* requires screening of all foreign correspondent bank accounts and also requires enhanced due diligence for accounts in the name of a foreign bank operating under an offshore banking license. Financial institutions subject to the law must demonstrate compliance and be able to respond to official requests for information and account documentation within certain prescribed time limits (generally, 120 hours). The advent of electronic banking has considerably heightened the complexity of know your customer issues. An August 15, 2001, SR Letter 01-20 *FFIEC Guidance on Authentication*, addresses the risks and risk management controls needed to authenticate the identity of e-banking customers.⁵ However, the underlying need for actual knowledge of the customer transcends the technical problems of transaction authentication.

International Cooperation

It might appear at first glance that the increasingly severe regulations applicable to U.S. financial institutions will create a competitive disadvantage vis-à-vis institutions operating in countries

⁵ See SR 01-20 *FFIEC Guidance on Authentication*, at < www.federalreserve.gov/boarddocs/SRLETTERS/2001/sr0120.htm>.

with strict bank privacy laws that tend to shield criminal activity from official detection. While there may be some temporary regulatory incongruity, there are strong efforts in enlightened foreign jurisdictions to effect changes that might result in a more level playing field. In the global scheme of things, FinCEN is one of 58 Financial Intelligence Units (FIU) that comprise the Egmont Group.⁶ These FIUs meet to exchange information and to provide training in support of their respective governments’ efforts to stop financial crime.

The OECD has sponsored the Financial Action Task Force on Money Laundering (FATF), notable for its list of Non-Cooperative Countries and Territories (NCCTs) with critical weaknesses in anti-money laundering systems.⁷ The FATF regularly reviews the NCCT list, and adds and deletes countries and territories as warranted. Notably, in June 2001, the FATF removed the Bahamas, Cayman Islands, Liechtenstein, and Panama from the NCCT list, while adding five other countries.⁸

The 31 FATF members, together with 18 regional bodies and observers, met

⁶ See the Egmont Group’s web site at < www1.oecd.org/fatf/Ctry-orgpages/org-egmont_en.htm>.

⁷ See the Financial Action Task Force’s web site at < www1.oecd.org/fatf/index.htm>.

⁸ See the FATF’s list of NCCTs and criteria for defining NCCTs at < www.fatf-gafi.org/NCCT_en.htm>.

at the end of October and agreed to expand the FATF mission to participate in the worldwide effort to combat terrorist financing. The Special Recommendations on Terrorist Financing emanating from this meeting commit the members to implement new international standards intended to deny terrorists and their supporters access to the international financial system. These standards are:

- Take immediate steps to ratify and implement the relevant United Nations instruments
- Criminalize the financing of terrorism, terrorist acts, and terrorist organizations
- Freeze and confiscate terrorist assets
- Report suspicious transactions linked to terrorism
- Provide the widest possible range of assistance to other countries’ law enforcement and regulatory authorities for terrorist financing investigations
- Impose anti-money laundering requirements on alternative remittance systems
- Strengthen customer identification measures in international and domestic wire transfers
- Ensure that entities, in particular non-profit organizations, cannot be misused to finance terrorism

The FATF also committed it self to closer cooperation and coordination with other organizations such as the UN and the Egmont Group. If the standards are adopted globally, the question of competitive disadvantage should be put to rest.

Clearly, there is a developing global consensus at both the public and private levels that the gloves need to come off in the fight against criminal use of the financial system. We encourage all Third District financial institutions to stay informed of

developments in this critical area and to implement best practices with respect to anti-money laundering and the detection of suspicious activities.

If you have any questions on the new anti-money laundering requirements, please contact your institution's central point of contact at the Federal Reserve Bank of Philadelphia. Alternatively, you can contact William Brown (William.J.Brown@phil.frb.org) at 215-574-7291. ■

Additional Sources of Information

Web Sites

Financial Crimes Enforcement Network (FinCEN) - www.treas.gov/fincen/
Financial Action Task Force (FATF) - www1.oecd.org/fatf/index.htm
Federal Financial Institutions Examination Council (FFIEC) - www.ffiec.gov/
Financial Intelligence Units (FIU) - www.ustreas.gov/fincen/int_fius.html
Office of Foreign Asset Control (OFAC) - www.treas.gov/ofac/

Federal Reserve Sources

Bank Secrecy Act Examination Manual - www.federalreserve.gov/boarddocs/supmanual/default.htm#bsaman
SR 01-23 Reporting Suspicious Transactions Relating to the Recent Terrorist Attacks to Law Enforcement
SR 97-19 Private Banking Activities
SR 96-5 Anti-Money Laundering Controls in Foreign Offices of U.S. Banks
SR 95-10 Payable Through Accounts
All SR Letters are available at <www.federalreserve.gov/boarddocs/SRLETTERS/>

Other Sources

Basle Committee - www.bis.org/
Committee of Ministers of the Council of Europe - www.europa.eu.int/scadplus/leg/en/lvb/l24016.htm
United Nations Office for Drug Control and Crime Prevention - www.undcp.org/money_laundering.html

“Fraud Prevention” *continued from page 5*

counts of this nature will be closed and a new account issued.

- A participating merchant contacts the Fraud Prevention Department to report suspicious or unusual accountholder behavior or related charges. If the accountholder is present at the merchant location or point of sale, the fraud prevention analyst will verify security information with the accountholder. If the information provided is correct, the fraud prevention analyst will either provide the merchant with

block will be placed on the account until a fraud prevention analyst can make a final determination regarding the validity of the accountholder’s claim.

Contact with the Accountholder.

Upon receiving a fraud alert, the fraud prevention analyst typically contacts the accountholder to verify account activity using automated or manual voice messages and form letters sent to the billing address on the account.

When receiving an inbound call from an accountholder, the analyst will

possible fraudulent activity and to determine the exact identity of a particular caller. Similarly, analysts may employ aided recall and coaching techniques to assist an accountholder in the verification process.

Accountholder Affidavit. As part of the fraud investigation process, a pre-filled affidavit is often forwarded to the primary accountholder for completion and signature. This affidavit is a legally binding document used by fraud investigators and criminal prosecutors to verify accountholder security information and to secure further details surrounding the fraud perpetrated. The format and text of the affidavit depend upon the type of fraud perpetrated, the individuals or organizations involved, and the preferences of the individual issuer. Affidavits are also used extensively for merchant chargeback purposes, as well as for the enforcement of agreements with suspects who want to make restitution in exchange for the cessation of criminal prosecution.

Completing the Investigation. To facilitate the decision-making process, pre-set actions are defined for the fraud prevention analyst. These actions provide guidance, but still allow analysts to use their judgement to address potentially fraudulent situations. Although not exhaustive, actions available to a fraud analyst after review of an account might include:

- Placing the account in a separate queue to monitor ongoing activ-

Analysts are intuitively skeptical of fraud claims and are encouraged to ask probing questions to determine the intent of each telephone call.

an authorization number or transfer the accountholder to a customer service representative to complete the transaction. If the accountholder is not present at the point of sale, a temporary block will be placed on the account until a fraud prevention analyst can contact the accountholder to verify the activity in question.

- An accountholder contacts the Fraud Prevention Department to inform them that their account has been compromised in some way. A temporary or permanent

first verify certain security information appearing on the account. After securing this preliminary identifying information, the fraud prevention analyst uses a pre-determined list of questions designed to support the Fraud Prevention Department’s efforts to identify and prohibit unauthorized activity efficiently, rapidly, and consistently. Analysts are intuitively skeptical of fraud claims and are encouraged to ask probing questions to determine the intent of each telephone call. It is not unusual for fraud prevention analysts to use subterfuge in their line of questioning to elicit concealed facts surrounding

ity or unusual authorizations

- Reviewing the account with no further action taken by the analyst
- Temporarily blocking the account, with a request that the accountholder present positive identification at the point of sale
- Permanently blocking the account, with a request that the accountholder fax positive identification to the Fraud Prevention Department for further review

When the fraud prevention analyst completes a fraud report, explanatory comments and specific codes are normally included in the report to assist in the fraud investigation. If the account is closed, the fraud prevention analyst will forward a replacement card with a new account number to the billing address appearing on the account within seven to ten days after completing a fraud report. If it is determined that the risk of future fraud losses involving the accountholder is too great, the fraud prevention analyst may decide against the issuance of a replacement card.

Credit Reporting Bureaus and Law Enforcement. Accountholders victimized by fraud are advised to contact the fraud victim assistance departments of the three major credit reporting bureaus to request that a “hawk alert” be placed on their credit reports. By completing this important step, the accountholder’s credit report will be monitored for signs of suspicious activity and unusual inquiries. Accountholders are also encouraged to file a criminal complaint with their local law

enforcement office to facilitate the investigation process.

Consumer Liability

The rights and responsibilities of parties engaged in electronic fund transfers are addressed in the *Electronic Fund Transfer Act of 1978* (“the Act”). The Federal Reserve’s Regulation E is the enabling regulation through which the Act is enforced. Under the provisions of the Act, consumer liability associated with unauthorized electronic fund transfers is generally limited to \$50 per fraud instance. Unlike their brick and mortar counterparts, e-merchants are fully liable for losses incurred from payment card fraud.

With the continued increase in consumer debt and the current weakness in the economy, the Fraud Prevention Department will likely continue to play an important role in the overall success of financial institutions for the foreseeable future.

In April 2000, Visa went beyond the current legal framework to introduce its “Zero Liability” policy. Under this policy, accountholders are held to a zero liability standard for unauthorized charges. MasterCard International complies with the Act and limits consumer liability to \$50.

In the majority of fraud cases, Visa and MasterCard hold the merchant, not the accountholder, responsible for fraudulent payment card activity. Using contractually agreed upon restrictions associated with monthly chargeback rates and volume, both Visa and MasterCard monitor merchant performance to ensure compli-

ance with acceptable limits.

Conclusion

The mission of the Fraud Prevention Department is to improve an issuer’s profitability by reducing fraud losses through the early detection and control of high-risk account activity. To accomplish this mission, today’s Fraud Prevention Department must create an environment that cultivates technological innovations, encourages synergetic initiatives, and adequately addresses a broad continuum of new service-related responsibilities including account retention, collections, and cross-selling. With the continued increase in consumer debt and the current weakness in the economy, the Fraud Prevention Department will

likely continue to play an important role in the overall success of financial institutions for the foreseeable future.

If you have any questions on fraud prevention measures for payment card operations, please contact Frederick W. Stakelbeck, Jr., Payment Card Analyst, (Frederick.W.Stakelbeck@phil.frb.org) at (215) 574-6422. ■



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!

Send an e-mail to Cynthia.Course@phil.frb.org to have your name added to the notification list.