Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Financial Institutions Required To Do Their Part To Fight Crime

This paper will briefly explain how the U.S. Patriot Act legislation came into existence, but its main focus will be to outline the requirements of the recently proposed Section 326 "Customer Identification Program." This paper will identify who must comply with the Section 326 ruling and will explore the impact it will have on day-to-day operations for financial institutions. It will familiarize the reader with some of the compliance software options available in the marketplace and in conclusion will evaluate the cos...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Financial Institutions Required To Do Their Part To Fight Crime

Terry Ritter

Practical Assignment Version 1.4b - Option 1
January 12, 2003

Abstract

Financial institutions have historically worked in tandem with governmental agencies to employ economic sanctions and freeze assets of those identified as being involved in criminal type activities. While crimes like identity theft have continued to rise over the last few years, financial organizations have struggled to balance risk with the services they are able to provide their customers. The recent downturn in the economy and the events of September 11, 2001 add even more pressure to the institutions already struggling to maintain revenues and retain their customer base.

This paper will briefly explain how the U.S. Patriot Act legislation came into existence, but its main focus will be to outline the requirements of the recently proposed Section 326 "Customer Identification Program." This paper will identify who must comply with the Section 326 ruling and will explore the impact it will have on day-to-day operations for financial institutions. It will familiarize the reader with some of the compliance software options available in the marketplace and in conclusion will evaluate the costs and public perceptions in an attempt to determine whether compliance with this legislation will be an effective defense in the struggle to stay one step ahead of the criminals.

Background

The need to verify a customer's identity is not a new concept to financial institutions. Banks and other financial entities have long maintained verification procedures as part of a strategy to prevent their organization from being involved in a fraudulent or criminal transaction. The Office of Thrift Supervision (OTS), created in 1989 as a result of the Financial Institutions Reform, Recovery, and Enforcement Act, is an agency of the United States Treasury Department. Its main function is to regulate federally charted savings and loan associations. OTS maintains its recommendations for account administration procedures as part of its published OTS Trust & Asset Management Handbook (http://www.ots.treas.gov/DOCS/427000.PDF). This publication, intended for OTS auditors, provides guidelines and expectations for normal financial account activities such as account setup, account review, account termination, etc.

The 1990s presented a new challenge as *identity theft* became a buzzword and financial institutions were faced with deciding what their role would be as their customers sought answers in how to protect the information associated with their identities. During this decade, the Internet was rapidly expanding and financial institutions, anxious to have the competitive edge, began offering online services

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

to their customers. Those who engage in criminal activity however, wasted no time in conquering this new frontier. Criminals quickly targeted social security numbers as being the passport to establishing fraudulent online identities. This unique personal identifier, often printed on commonly used documents such as driver's licenses and personal checks, also became available for sale on the Internet. By 1998, the Identity Theft and Assumption Deterrence Act was enacted making identity theft a federal crime [FTC98]. By 2001, forty-six states followed suit and enacted identity theft laws of their own [BLO01]. While these laws have provided the legal recourse to prosecute perpetrators and compensate victims, their success in deterring the crime has been less than satisfactory. Identity theft has continued to rise at alarming proportions and has been called the fastest growing crime in our nation. During 2000, The Office of the Comptroller of the Currency (OCC), responsible for ensuring the soundness and safety of the U.S. banking system, received reports from 500,000 people indicating they were victims of identity theft [OCC01]. In May 2001, *USA Today* reported "nearly 2,000 consumers contact the Federal Trade Commission every week to report they've been victims of identity theft" and estimated the actual annual numbers could be as high as 750,000 victims [DUG01]. When Social Security Inspector General James Huse testified before the House Ways and Means subcommittee in May 2001, he called identity theft a "national crisis" [WAP01]. As financial organizations added identity theft to their growing 'watch list' and began evaluating their customer verification processes, a series of events would take place during the last few months of 2001 that would result in yet another change to their role and responsibilities.

Prior to the mind shift that evolved after the 9/11 terrorist attacks, consumers were becoming more familiar with their own privacy rights and the average American most likely would have perceived any increased scrutiny at their local bank as being unnecessary and intrusive.

As early as late 1998, the Office of Thrift Supervision, the Federal Reserve, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation combined their efforts and proposed "know your customer" requirements. Financial establishments complained en masse about the additional administrative overhead and argued they have long had procedures in place to comply with the Bank Secrecy Act[1]. Additionally, they expressed concerns that the measures that would need to be taken in order to increase the verification of the customer's identity could inhibit their compliance with the already enacted privacy requirements [PRI02]. By March of 1999, the regulatory agencies accepted defeat and the proposed "know your customer" ruling was withdrawn.

The September 11, 2001 attacks proved to be a wakeup call that resulted in each American having to re-assess and re-define acceptable boundaries between

1 The Bank Secrecy Act, passed in the 1970s, requires banks to record transactions in excess of $10,000 to a currency report.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

security and privacy. To those outside of the financial arena, the terrorist attacks on September 11 brought a new awareness of how inter-related financial transactions are to the activities of terrorist groups. While the general public may have become aware of these issues for the first time shortly after the September 11 disaster, financial organizations and politicians had been struggling for years to agree on whether more stringent identification measures were necessary.

As the post-September 11 investigations got underway, evidence was obtained that indicated the terrorists had previously integrated themselves into our culture by virtue of establishing residency, securing employment and obtaining American bank accounts. *Newsweek* reported "banks had been reporting suspicious account activity to the government long before evidence emerged that the terrorists involved in the September 11 attacks may have used U.S. accounts to help fund their activities" [BARa02]. Although banks and other financial institutions sought to portray an image of full cooperation, the 1999 defeat of the proposed 'know your customer' ruling bears record to the fact that they did not support legislation being passed that would obligate them to implement more stringent account procedures.

With the increase in public support and a new sense of urgency, the federal government wasted no time in acknowledging its goal to find solutions that would identify and restrict criminal activities such as money laundering and terrorist group funding. Two weeks after the September 11 terrorist attacks, President Bush stated, "We will direct every resource at our command to win the war against terrorists, every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence. We will starve the terrorists of funding" [USEa02].

The previously defeated efforts of the combined financial regulatory agencies provided a strong foundation as governmental agencies joined forces and seized the opportunity to have stricter financial regulations enacted once and for all. New representation from the Securities and Exchange Commission (SEC), the National Credit Union Administration (NCUA), and the Financial Crimes Enforcement Network - part of the Treasury Department (FinCEN) combined with those involved in the previous efforts (i.e. the Office of Thrift Supervision, the Federal Reserve, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation) to round out the new taskforce. Additional guidance on money laundering was obtained from the Financial Action Task Force (FATF). The recommendations of the FATF were subsequently presented to the United Nations (U.N.) in an effort to rally international support for abolishing money laundering and terrorist funding worldwide. Since then the FATF's suggestions have become an unofficial international standard that other nations are following to ensure the safety of their own financial systems.

With the backing of the U.S. House of Representatives and the U.S. Senate, President Bush, on October 26, 2001, signed into law the U.S.A. Patriot Act.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

More than just a timely title, the U.S.A. Patriot Act is actually an acronym that stands for "The Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" [EFF01]. This legislation, like no other before it, encompasses all financial organizations. Most of the previously passed federal legislation related to a specific sector of the financial industry (i.e. banks, credit card issuers, credit unions, brokerage firms, etc.) This new comprehensive anti-terrorism legislation has major impacts to the financial industry. Even though the U.S.A. Patriot Act is divided into multiple sections, each with its own mandated deadline, the schedule is very aggressive with the full implementation initially targeted for completion by the end of 2002 For the purposes of this paper, the focus will be limited to exploring Section 326, entitled as the 'Customer Identification Program.' To read an overview of the entire U.S.A. Patriot Act, section by section, refer to "The 2001 Patriot Act and Its Implications for the IT Security Professional" in the SANS Reading Room. http://rr.sans.org/legal/patriot_act2.php

Section 326 – Customer Identification Program

On July 17, 2002 the Office of Public Affairs, a division of the U.S. Treasury Department, in a joint release with seven contributing financial regulatory agencies, published the long awaited details of the proposed ruling Section 326. The official announcement stated its purpose and clearly identified who would be impacted:

> "The proposed rules seek to protect the U.S. financial systems from money laundering and terrorist financing. Additionally, by requiring identity verification procedures for all new accounts opened after the effective date of the final rules, the rules could also protect consumers against various forms of fraud, including identity theft. The proposed rules outline requirements for the following financial institutions: banks and trust companies, savings associations, credit unions, securities brokers and dealers, mutual funds, futures commission merchants, and futures introducing brokers." [USDa02]

Financial organizations were given until September 6, 2002 (approximately 45 days) to submit their written comments and concerns. Initially, the U.S. Treasury Department set an effective date of October 25, 2002 but due to the outpouring of concerns they received, the October 25th effective date has been rescinded and as of yet, a new effective date has not been established. The official postponement announcement released on October 11, 2002 from the Office of Public Affairs, indicated the final ruling would provide financial organizations "a reasonable amount of time" to comply and promised additional guidance would soon be issued. [USDb02] In order to understand some of the concerns that were raised, we must first examine the details of what is included in the original proposed ruling.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Section 326 proposal can be grouped into the following basic requirements:

1) Establish a Customer Identification Program (CIP)
2) Obtain identity verification information
3) Verify customer's identity information
4) Compare customer's identity to government list of known or suspected criminals
5) Store identity verification information

Realizing it would be impossible to dictate a detailed approach that could be flexible enough to integrate into the varied operations represented throughout the many sectors of the financial industry, the Section 326 ruling sought to establish a set of minimum requirements that could be adapted to the way each individual sector conducted business. The proposed ruling acknowledges each business has different exposures and therefore supports a risk-based approach using the following considerations:

1. The size of the business
2. The type of business
3. The account types offered
4. The methods available for opening accounts

Unlike other sections of the U.S.A. Patriot Act, Section 326 limited the scope of its customer identification requirements to 'new' accounts and did not impose any retroactive provisions. The definition of what constituted a 'new account' however, was broadened to include some common account activities such as adding a new signatory to an existing account. Generally speaking, if a change is made to an existing account, most likely it would be subject to the new requirements. There are also some distinctions made between U.S. citizens and non-U.S. citizens as well as differences in what is required of an individual versus a corporation.

1. Establish Customer Identification Program

In order to demonstrate its compliance with each of the requirements listed above, every financial organization is required to have a Customer Identification Program (CIP). The CIP is required to be a written document, formally reviewed and approved by the financial organization's internal board of directors or governing entity. The CIP should provide detailed information demonstrating how the financial institution and any subsidiaries comply with each component of the Section 326 ruling. For example, the CIP should address items such as refusing to open an account in situations where the customer cannot provide appropriate identification information. The CIP must include internal policies and procedures and must designate a compliance officer who will be required to verify the necessary controls are in place to ensure ongoing adherence to the ruling. Furthermore, the CIP should outline internal auditing processes and an

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

employee-training program. The employee-training program will be a very important element and can help the organization show due diligence as they work to implement the new rules. The CIP should not be considered as a standalone entity but should rather support the already existing requirements of the Bank Secrecy Act. For financial institutions subject to OTS audits, the OTS has already modified their checklists to include verifying the existence of a CIP. Once the new Section 326 ruling becomes effective, OTS auditors will begin evaluating the financial organization's compliance with each element of the Section 326 ruling. Financial institutions found in non-compliance will incur large civil and possibly criminal penalties and fines.

2. Obtain identity verification information

People intent on committing fraudulent transactions often rely on tactics that contribute to others being distracted from their normal procedures. Financial institutions have long trained their employees to be watchful of people who show up right before closing time trying to rush thru normal account opening processes. Obtaining the appropriate identity information prior to opening an account will now be an audited event. Though financial companies already collect identity information as part of their normal account opening processes, this practice will now be extended to encompass other innocuous account activities such as when an existing customer wants to add another signatory to their account.

Required identity information includes the customer's name, address, date of birth and an identification number. The identity items provided must be officially recognized documents such as a current drivers license. For U.S. citizens, the identification number can be a social security number. Non-U.S. citizens will need to produce a similar number from a government-issued document that certifies their nationality of residence and bears a photograph (i.e. alien identification card number or passport number).

The proposed Section 326 ruling requires financial institutions to notify their customers of the new identification requirements. The notification should help the customer understand why they are obligated to provide the identification information. Acceptable notification methods include verbally explaining the requirements to the customer, electronic notification on the institution's website (for online accounts), and written notification such as brochures or lobby posters available for potential customers to review.

3. Verify customer's identity information

Although the ruling dictates that the customer's identity information must be collected prior to opening a new account, the new ruling allows financial institutions the flexibility of performing the verification of the information within a reasonable timeframe either before or after the account is opened. This will

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

allow each financial entity to integrate compliance procedures into their daily operations while minimizing the impact to their customers. Customers opening their account in person will be required to provide the actual identity documents. This will allow the institution to retain a copy of the documents used to verify the customer's identity. To handle situations where the customer is unable to provide the required documentation in person (i.e. opening an online account), the ruling allows the usage of non-documentary verification. Non-documentary verification methods could include comparing the customer provided information with a credit report or financial statement, making phone calls to check references, using software to consult public databases, etc.

The CIP should outline specifics regarding the customer's use of the account during the verification process. This would include scenarios like whether the customer is able to complete transactions during the verification process, what circumstances will dictate an account being closed, etc.

4. Compare customer's identity to government list of known or suspected criminals

Once the customer's identity information has been obtained and verified, the financial institution is then required to compare the information to a U.S. government produced listing of known or suspected terrorists and terrorist organizations. The ruling also requires that the CIP include procedures for handling a positive match. Each of the lists below outlines the financial institution's responsibility when a suspect situation is detected. Failure to follow the procedures is considered a serious offense and could result in criminal prosecution. At this time, the proposed Section 326 ruling doesn't specify a certain list that must be used. This issue was one of the contributing factors that lead to the delay of the ruling being implemented. Most financial institutions have expressed a desire to have the government designate one list as the authoritative source. Some of the lists currently available for use are:

- The Federal Bureau of Investigation (FBI) Control list
- Specially Designated Nationals and Block Entities (SDN-BE) list
- Office of Foreign Assets Control (OFAC) list

The U.S. government has maintained these lists for years and even though the lists have always been available to financial institutions, until now it has not been a requirement for them to regularly use the listings. In the past, financial organizations would periodically screen customers or certain transactions but rarely compared their entire account database.

Although the Section 326 proposal hasn't yet dictated a single authoritative source for comparing each customer's identity, Goldman Sachs has already partnered with Citigroup, Merrill Lynch and about twenty of the world's largest financial institutions to setup DataCorp International, a private database

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

company. Sources involved in this effort indicate the initial data has been accumulated from public sources and contains approximately three million files on entities with known ties to terrorist or other criminal activity. Similarly, British-based World Check, Inc. formed two years ago, offers their clients a compliance database with half a million hyperlinks to information sources [BARb02].

In a later section, this paper will explore some of the compliance software available to help financial institutions meet this new requirement.

5. Store identity verification information

The proposed Section 326 ruling mandates that each financial institution store the identity verification documents for a period of at least five years after the customer's account is closed. Specifically the stored records must include copies of each item that was collected and used in the verification of the customer's identity. For example, if the customer presented their drivers license as proof of their identity, then the financial institution would be required to make a readable photocopy of the drivers license and that photocopy would need to be retained for a period of at least five years after the customer's account is closed. If a non-documentary method were used such as obtaining a credit report, then a copy of the credit report used would need to be retained for the specified period.

Additionally, the ruling specifies that if a discrepancy is found between the information that the customer provided and the information used in the identity verification, then the financial institution must document whether the discrepancy was resolved and if so, what means did the financial institution use to ensure they knew the true identity of the individual. The discrepancy related information would then become part of the identity record and would also be subject to the five-year retention period. The CIP should include documentation related to this mandated recordkeeping and should outline procedures for specific scenarios such as how discrepancies are to be handled.

This recordkeeping requirement has generated an outcry of complaints from financial institutions. Besides concerns over logistical items such as the overhead that each financial organization will incur to physically store the documents, many argue that keeping the identity information for five years after the closing of an account is excessive and unnecessary especially for financial organizations that have a high turnover of accounts such as an investment company who engages in thousands of online transactions. Others have voiced concerns that imaging identity items that contain a photo id such as a driver's license will make them vulnerable to accusations of violating the Equal Credit Opportunity Act (ECOA), which prohibits discrimination on the basis of factors such as sex and race. How these concerns will be addressed and resolved is still an outstanding item.

Compliance Solutions

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Since July 2002, financial organizations have been scrambling to prepare for the upcoming Section 326 requirements. Although the financial industry and the American public have been slow to accept the idea that additional federal regulation is really necessary, initial polls have shown that the tide of support is shifting. The publicity of terrorist funding and fast growing crime such as identity theft continues to raise public awareness and helps foster a better understanding and acceptance for implementing a new approach.

In August 2002, a survey of financial industry professionals was conducted by eFunds, a leading provider of financial information solutions and business technology. The survey results indicate 70% of its participants support the U.S.A. Patriot Act and believe it will deter terrorist financing and money laundering. The survey asked, "What else, if anything, needs to be done to prevent terrorist access to the U.S. financial system?" Approximately 33% said 'more diligence was needed by the staff' and 20% said 'more employee training is required.' Seventy-two percent cited 'better technology in the hands of criminals' as the reason for the increase in fraudulent activities while only 5% blamed internal controls. Lisa Nelson, Chief Privacy Officer for eFunds Corporation, stated:

> "It's encouraging to see the confidence that financial institutions place in the PATRIOT ACT. But simply passing new regulations cannot by itself keep the financial system safe. Organizations have to be diligent about implementing the new rules and carefully following each step in the account-opening process. With new technology, it's certainly a challenge to stay one step ahead of the terrorists and criminals. But eFunds is committed to partnering with the industry to continually develop new tools in the fight against fraud and to serve as a resource for PATRIOT ACT compliance." [EFC02]

The aggressive timeframe and complexity of the Section 326 requirements has resulted in many financial institutions looking outside of their organization for compliance solutions. This is definitely good news for companies offering compliance software and consulting services. A wide range of services is available from overall compliance consulting to assistance with specific items such as creating a written CIP for a financial institution. An even larger range of software is available, some with customizable web interfaces to monitor daily account activity, perform real-time reporting, consolidate customers' history, screen daily transactions for unusual events, and provide a data repository, etc. While some companies have chosen to specialize in one compliance area, others have taken a one stop shopping approach and offer a comprehensive suite of products to ensure compliance with all the U.S.A. Patriot Act requirements. The list below provides a starting point of companies who offer compliance related services and software solutions. For additional information, please click on the hyperlinks:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Concord EFS, Inc – known for being a leader in processing electronic commerce transactions, Concord EFS, Inc. utilizes its Primary Payment Systems, Inc. subsidiary to provide a suite of Early Warning Solutions including IDENTITY CHEK, DEPOSIT CHEK, PRIME CHEK and STAR CHEK. Although IDENTITY CHEK has been available for over 15 years, it has been extensively tested during the last twelve months on over 27 million account openings to ensure it can detect irregularities in an individual's identification information.
Primary Payment Systems, Inc.

EFunds – formerly part of the Deluxe Corporation, eFunds offers integrated electronic fund network solutions for financial services companies and retailers. Delivering a comprehensive solution, eFunds offers a suite of products and services including ChexSystems, FraudFinder, Audit Report, QualiFile and OFAC Screening to ensure compliance with each requirement of the Section 326 ruling. eFunds

Mantas – a spin-off company from SRA International and its partner, Safeguard Scientifics, Inc., Mantas provides sophisticated behavior detection technology that allows financial institutions to globally analyze their customer account information on a per transaction basis to detect suspicious activity. With clients such as the National Association of Securities Dealers (NASD), Citigroup and Merrill Lynch, Mantas boasts its software is capable of handling "more than 300 million transactions per day." Mantas

Penley – offers digital certificate based eFinance identity verification and risk management solutions for small to mid-size banks and brokerage firms. Penley's software products (FastLoan, FastPass, FastTransfer and eCorrespondence) are each designed to meet a specific financial industry need. The newest product rounding out Penley's software suite is FastWatch, a product designed to assist financial institutions in complying with the Section 326 requirements. FastWatch offers a customizable CIP policy, the ability to verify a customer's identity using public databases, checking the customer's identity against a government designated list of known or suspected terrorists, as well as data storage and reporting capabilities. Penley claims FastWatch will provide an 'immediate response' in identifying people or organizations whose transactions should be flagged or blocked. Penley

Sybase – claiming that fifty-six percent of Wall Street firms rely on their technology products and services, Sybase is an infrastructure software company that touts its ability to integrate solutions on disparate enterprise platforms with its "everything works better when everything works together" slogan. To assist financial organizations with complying with

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

U.S.A. Patriot Act requirements, Sybase offers PATRIOTcompliance Solution, an "end to end solution to address the significant data management, integration and reporting challenges the financial services industry faces in complying with the USA PATRIOT Act of 2001."
Sybase

Vastera – established in 1992, Vastera initially focused on providing export management solutions. Since then, Vastera has expanded to offer 'state-of-the-art technology' and has established themselves as a leader in navigating the myriad of international trade regulations. Clients such as Ford Motor Company and IBM Corporation look to Vastera to move their products and information across international boundaries. Vastera's Homeland Security package includes a detection and verification component to assist their customers with U.S.A. Patriot requirements.
Vastera
Vastera Homeland Security

Conclusion

The Section 326 proposal, along with the other U.S.A. Patriot Act requirements, demonstrate that protecting the integrity of the U.S. financial systems has become part of the national agenda. The U.S. government and the financial industry have long understood how inter-dependent they are in fighting both the ordinary individual intent on committing identity fraud by opening an account using a fake name and social security number to the large scale international terrorists who use our American banking system and other shell banks to transfer funds worldwide.

While skeptics and some of the American public wonder whether these new identity requirements will be an effective deterrent in fighting terrorism and fraud related crime like identity theft, financial institutions, already absorbing an estimated $120 million in compliance related costs [BARc02], are desperate to find solutions to offset their ever increasing fraud related losses.

Celent Communications, a financial services consulting and research firm, estimates in the next three years, U.S. financial institutions will sustain losses of more than $8 billion a year due to identity theft alone [CEL01].

Though many claim it is too early to know whether the new technology and regulations will narrow the funding opportunities for terrorists, others like Kenneth W. Dam, Deputy Secretary of the Treasury, are convinced that the U.S. is leading the way in globally stopping terrorist funding. In a recent speech before the Senate Banking Committee, Kenneth said,

> "Our priority is to help prevent terrorist attacks by disrupting terrorist finances. As the President has said, we seek to 'starve the terrorists of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

> funding.' Our goal is to deprive terrorists of one of the raw ingredients in terrorism: money for arms, explosives, plane tickets, and even the day-to-day sustenance of operatives. We believe from our intelligence channels that Al Qaeda and other terrorist organizations are suffering financially as a result of our actions. We also believe that potential donors are being more cautious about giving money to organizations where they fear that the money might wind up in the hand of terrorists." [USEb02]

During the same speech, Kenneth states that the United States has received a "remarkable degree of cooperation" from foreign governments with participation from 147 countries and reports "Since September 11th, the United States and other countries have frozen more than $80 million in terrorist-related assets." [USEc02]

In contrast with the U.S. government's enthusiasm, the financial industry, though supportive of the government's overall plan, believes more work is needed to define the specifics of the Section 326 ruling. In September of 2002, the Financial Services Roundtable, an organized group representing more than 100 of the largest financial services companies, submitted its comment letter to the Financial Crimes Enforcement Network. In it, the Roundtable says it "strongly supports the federal government's efforts to combat money laundering and related activities that help finance global terrorism" and that it "applauds the efforts of Treasury and the agencies to devise a uniform set of rules that apply to all financial industry participants." [WHI02] The comment letter however, goes on to point out several specific areas where additional clarification is needed such as dealing with safety deposit boxes, rules for one-time transactions, consistency in the definition of a customer, handling authorized signatories for corporate accounts and the Roundtable even requests excluding certain individuals such as beneficiaries. The Roundtable also brings up concerns with potentially violating consumer's privacy rights as well as apprehensions about the financial institution's adherence to the Fair Credit Reporting Act.

After obtaining the input from the financial industry, the U.S. Treasury Department issued a press release on October 11, 2002 stating financial institutions "will not be required to comply with section 326 of the USA Patriot Act or the proposed rules issued by the Treasury and the federal functional regulators on July 23 until final implementing regulations are issued and become effective" and that "the final rules will provide financial institutions with a reasonable amount of time in which to come into compliance" [USDc02]. The U.S. Treasury Department also says that financial institutions should already be taking basic steps to ensure appropriate customer identification.

Although the specific requirements for the Section 326 ruling are not fully defined and even though the debate of cost versus benefit will continue indefinitely in the financial and public arenas, no one can deny that difficult times call for difficult measures. Kenneth Dam, Deputy Secretary of the Department of the Treasury

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

sums it up well in his January 29, 2002 testimony before the United States Senate as he reflected on the post-September 11 efforts.

> "The government and the financial community were forced to rethink assumptions, to reevaluate risks of money laundering and abuse in connection with terrorist financing, and, ultimately, to take the steps necessary to protect the country's financial system. This is an unconventional war where there are no boundaries, where civilians are the targets, where people (or so-called 'martyrs') are the weapons, and where electronic money transfers and messaging are the fuel and the logistics train. Among other things, identifying the flow of money helps us find the footprint of sleeper cells, disable them, and perhaps prevent the next attack." [USEd02]

References

[FTC98]
Federal Trade Commission (FTC); "Identify Theft and Assumption Deterrence Act"; October 1998; FTC website URL:
http://www.ftc.gov/os/statutes/itada/itadact.htm

[BLO01]
Block, S.; "States do their part to squash identity theft"; August 2001; USA Today website URL: http://www.usatoday.com/money/general/2001-08-10-identity.htm

[OCC01]
Office of the Comptroller of the Currency (OCC); "OCC Issues Advisory on Identity Theft and Pretext Calling"; April 2001; OCC website URL:
http://www.occ.treas.gov/ftp/release/2001-41.doc

[DUG01]
Dugas, C.; "Identity theft on the rise"; May 2001; USA Today website URL:
http://www.usatoday.com/money/perfi/general/2001-05-11-identity-theft.htm

[WAP01]
Washington Associated Press (WAP); "Radical solutions eyed in Net identity theft battle"; May 2001; USA Today website URL:
http://www.usatoday.com/tech/news/2001-05-23-id-theft-solutions.htm

[PRI02]
Pringle, L.; "Management and Board of Directors' Responsibilities to Oversee 'Know Your Customer' Requirements of the USA PATRIOT Act"; June 2002; Compliance Headquarters website URL:
http://www.complianceheadquarters.com/Special_Reports/management_and_board_of_directors_responsibilities.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[BARa02]
Barrett, J.; "Banking on Software Solutions"; June 2002; MSNBC website URL: http://www.msnbc.com/news/766013.asp?cp1=1

[USEa02]
United States Embassy (USE); "U.S. Says Global Help is Key to Stopping Terror Funds"; January 2002; U.S. Embassy website URL: http://usembassy.state.gov/tokyo/wwwhse0987.html

[EFF01]
Electronic Frontier Foundation (EFF); "USA PATRIOT Act as Passed by Congress"; October 2001; EFF website URL: http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011025_hr3162_usa_patriot_bill.html

[USDa02]
United States Department of Treasury (USDT); "Treasury and Federal Financial Regulators Issue Patriot Act Regulations on Customer Identification"; July 2002; USDT website URL: http://www.ustreas.gov/press/releases/po3263.htm

[USDb02]
United States Department of Treasury (USDT); "Treasury Department Provides Guidance on Compliance with Section 326 of USA PATRIOT ACT"; October 2002; USDT website URL: http://www.treas.gov/press/releases/po3530.htm?IMAGE.X=21\&IMAGE.Y=8

[BARb02]
Barrett, J.; "Banking on Software Solutions"; June 2002; MSNBC website URL: http://www.msnbc.com/news/766013.asp?cp1=1

[EFC02]
eFunds Corporation; "eFunds Survey Shows Financial Industry Confident USA PATRIOT ACT Will Help Protect Financial System from Terrorists"' August 2002; eFunds Corporation website URL: http://www.corporate-ir.net/ireye/ir_site.zhtml?ticker=EFDS&script=410&layout=-6&item_id=326178

[BARc02]
Barrett, J.; "Banking on Software Solutions"; June 2002; MSNBC website URL: http://www.msnbc.com/news/766013.asp?cp1=1

[CEL01]
Celent Communications; "Identity Theft: Impact on the Financial Services Industry"; September 2001; Celent Communications website URL: http://www.celent.com/PressReleases/20010904/IdentityTheft.htm

[USEb02]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

United States Embassy (USE); "U.S. Says Global Help is Key to Stopping Terror Funds"; January 2002; U.S. Embassy website URL:
http://usembassy.state.gov/tokyo/wwwhse0987.html

[USEc02]
United States Embassy (USE); "U.S. Says Global Help is Key to Stopping Terror Funds"; January 2002; U.S. Embassy website URL:
http://usembassy.state.gov/tokyo/wwwhse0987.html

[WHI02]
Whiting, R.; (Letter to Financial Crimes Enforcement Network); September 2001; The Financial Services Roundtable website URL:
http://www.fsround.org/PDFs/1958RevisedFSRCommentLetterreSection326v2.pdf

[USDc02]
United States Department of Treasury (USDT); "Treasury Department Provides Guidance on Compliance with Section 326 of USA PATRIOT ACT"; October 2002; USDT website URL:
http://www.treas.gov/press/releases/po3530.htm?IMAGE.X=21\&IMAGE.Y=8

[USEd02]
United States Embassy (USE); "U.S. Says Global Help is Key to Stopping Terror Funds"; January 2002; U.S. Embassy website URL:
http://usembassy.state.gov/tokyo/wwwhse0987.html

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced