

May 2005

USA PATRIOT ACT

Additional Guidance Could Improve Implementation of Regulations Related to Customer Identification and Information Sharing Procedures



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-05-412](#), a report to congressional requesters

Why GAO Did This Study

Title III of the USA PATRIOT Act of 2001, passed after the September 11 terrorist attacks, amended U.S. anti-money laundering laws and imposed new requirements on financial institutions. Section 326 of the act required the development of minimum standards for verifying the identity of financial institution customers. Section 314 required the development of regulations encouraging the further sharing of information between law enforcement agencies and the financial industry and between the institutions themselves. Because of concerns about the implementation of these new provisions, GAO determined how (1) the government developed the regulations, educated the financial industry on them, and challenges it encountered; (2) regulators have updated guidance, trained examiners, and examined firms for compliance; and (3) the new regulations have affected law enforcement investigations.

What GAO Recommends

To help financial institutions implement their CIPs, GAO recommends that Treasury, through FinCEN and with the federal financial regulators and SROs, develop additional guidance on ongoing implementation issues. To improve examinations of compliance with CIP, GAO also recommends that FinCEN work with the federal financial regulators to develop additional guidance for examiners. Treasury agreed with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-412.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Yvonne Jones at (202) 512-2717 or jonesy@gao.gov.

USA PATRIOT ACT

Additional Guidance Could Improve Implementation of Regulations Related to Customer Identification and Information Sharing Procedures

What GAO Found

Treasury (including its Financial Crimes Enforcement Network (FinCEN)), the federal financial regulators, and self-regulatory organizations (SRO) overcame challenges to create regulations that apply consistently to a diverse financial sector and have used several outreach mechanisms to help the financial industry understand and comply with Customer Identification Program (CIP) requirements under section 326 and information sharing requirements under section 314. However, several implementation challenges remain. Industry officials told us some of their concerns have been addressed but they are still concerned about (1) how some CIP requirements will be interpreted during compliance examinations, (2) the lack of feedback from law enforcement on information provided by financial institutions through section 314(a), and (3) the extent to which they can share information with each other under section 314(b).

The six federal financial regulators and five SROs in our review have issued examination guidance covering sections 326 and 314, subsequently trained examiners, and begun examining financial institutions for compliance with CIP and section 314. GAO's review of examinations showed progress, but coverage varied in part because the examinations were conducted during early implementation. One aspect of CIP that was not always covered in examinations was whether financial institutions had adequately developed a CIP appropriate for their business lines and types of customers. However, this aspect of CIP is critical for ensuring that the identification and verification procedures are appropriate for types of customers and accounts that are at higher risk of being linked to money laundering or terrorist activities. Some examinations also revealed implementation difficulties related to CIP that could lead to inconsistencies in the way examiners conduct examinations. For example, some examiners did not differentiate between the CIP requirement and other procedures that require customer identification information. Coverage in the examinations GAO reviewed of how institutions had implemented section 314 requirements was somewhat lower than for CIP, in part, because CIP received more attention from examiners and information sharing between financial institutions is voluntary. In the examinations GAO reviewed, apparent violations of the CIP requirement and section 314(a) regulations were mostly addressed through informal actions between the institution and the regulator.

Officials from the Department of Justice and other law enforcement agencies told us that CIP and section 314 have assisted them in the investigation of money laundering and terrorist financing cases. Some officials said that CIP has been useful because financial institutions have more information on their customers so they obtain more useful information when issuing grand jury subpoenas and other requests for information. Many officials said the 314(a) process had improved coordination between the law enforcement community and the financial industry and increased the speed and efficiency of investigations.

Contents

Letter

Results in Brief	1
Background	5
Developing Regulations for CIP and Section 314 That Applied to a Wide Range of Financial Institutions Was Difficult and Complex	9
Treasury and the Federal Financial Regulators Have Reached Out to the Financial Industry to Assist It in Implementing CIP and Section 314 Rules, but Industry Concerns Remain	11
Financial Regulators and SROs Have Updated Examination Guidance and Trained Examiners to Evaluate Compliance with CIP and Section 314	21
Examinations and Enforcement Actions Highlight Progress and Difficulties in Overseeing Compliance with the CIP Requirement and Section 314	28
Law Enforcement Officials Believe That Section 314(a) and CIP Have Been Valuable Tools in Terrorist and Money Laundering Investigations	36
Conclusions	59
Recommendations for Executive Action	62
Agency Comments and Our Evaluation	64

Appendixes

Appendix I: Scope and Methodology	67
Appendix II: Comments from the Department of the Treasury	71
Appendix III: Comments from the National Credit Union Administration	73
Appendix IV: Comments from the Securities and Exchange Commission	74
Appendix V: GAO Contacts and Staff Acknowledgments	76

Related Products

77

Tables

Table 1: Banking Regulators Anti-Money Laundering Training-2004	33
Table 2: Securities Regulators Anti-Money Laundering Training-2004	35
Table 3: Coverage of CIP in Our Sample of Examinations Conducted between October 1, 2003, and May 31, 2004	38

Table 4: Anti-Money Laundering Policies That Depend on Procedures to Verify Customer Identities	43
Table 5: Coverage of Section 314(a) in Our Sample of Examinations Conducted between October 1, 2003, and May 31, 2004	46
Table 6: Coverage of Section 314(b) in Our Sample of Examinations Conducted between October 1, 2003, and May 31, 2004	49
Table 7: Examples of Minor and Significant 314(a) Deficiencies and Violations Identified in the Sample	51
Table 8: Examples of Minor and Significant CIP Deficiencies and Violations Identified in the Sample	51
Table 9: Recent Enforcement Actions and Civil Money Penalties against Banks That Included CIP and Section 314(a) Violations	54
Table 10: Recent Enforcement Actions against Securities Broker-Dealers That Included CIP and Section 314(a) Violations	56
Table 11: Description of Our Approach for Sampling Examinations Covering CIP and Section 314	69

Figures

Figure 1: Key Dates in the Rulemaking Process for CIP	13
Figure 2: Requirements for Customer Identification and Verification Procedures	15
Figure 3: Key Dates of the Rulemaking Process for Section 314	18
Figure 4: The 314(a) Information Sharing Process after the Moratorium	19

Abbreviations

BSA	Bank Secrecy Act
CBOT	Chicago Board of Trade
CFTC	Commodity Futures Trading Commission
CIP	Customer Identification Program
CME	Chicago Mercantile Exchange
EOUSA	Executive Office for U.S. Attorneys
FAQ	Frequently Asked Question
FBI	Federal Bureau of Investigations
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
ICE	Immigration and Customs Enforcement
MOU	Memorandum of Understanding
NCUA	National Credit Union Administration
NFA	National Futures Association
NYSE	New York Stock Exchange
OCC	Office of the Comptroller of Currency
OFAC	Office of Foreign Assets Control
OTS	Office of Thrift Supervision
SAR	Suspicious Activity Report
SEC	Securities and Exchange Commission
SRO	Self Regulatory Organization
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, D.C. 20548

May 6, 2005

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
House of Representatives

The Honorable John N. Hostettler
Chairman
Subcommittee on Immigration, Border Security, and Claims
Committee on the Judiciary
House of Representatives

Following the terrorist attacks on September 11, 2001, Congress passed the USA PATRIOT Act (PATRIOT Act), arming the U.S. government with new tools for investigating terrorism and terrorist financing.¹ The passage of the PATRIOT Act was prompted, in part, by the enhanced awareness of the importance of combating terrorist financing as part of the U.S. government's overall anti-money laundering efforts, because terrorist financing and money laundering can involve similar techniques and use the U.S. financial system to support criminal activity. Title III of the PATRIOT Act amended the Bank Secrecy Act² (BSA)—the key statute that governs the U.S. government's anti-money laundering regulatory structure. Two provisions of Title III—sections 314 and 326—were specifically highlighted by the National Commission on Terrorist Attacks Upon the United States (also known as the 9-11 Commission) in its report on terrorist financing as being important provisions in detecting and preventing terrorist financing. The Financial Crimes Enforcement Network (FinCEN), the federal financial regulators, and self-regulatory organizations (SRO) are

¹Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). We will refer to the act as the "PATRIOT Act".

²The body of law commonly referred to as the Bank Secrecy Act encompasses numerous provisions enacted by Titles I & II of Pub. L. No. 91-508, 84 Stat. 1114 (1970), and codified as amended at 31 U.S.C. §§ 5311-5332 and 12 U.S.C. §§ 1829b and 1951-1959. BSA requires reports and records of transactions involving cash, negotiable instruments, or foreign currency and authorizes the Secretary of the Treasury to prescribe regulations to ensure that adequate records are maintained of transactions that have a high degree of usefulness in criminal, tax or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities.

responsible for ensuring that the financial institutions comply with the BSA and BSA regulations through examinations and enforcement actions.³

Section 326 of Title III required the Secretary of the Treasury to develop regulations establishing minimum standards for financial institutions to follow when verifying the identity of its customers in connection with the opening of an account.⁴ In May 2003, the Department of the Treasury (Treasury), through FinCEN, and the federal financial regulators jointly adopted these regulations prescribed by section 326 regarding certain financial institutions.⁵ The compliance date for these new regulations was October 1, 2003. These regulations require financial institutions to establish a written customer identification program (CIP) that includes procedures for obtaining minimum identification information from customers that open an account with the financial institution, such as a person's date of birth, a government identification number, and physical address. The regulations stipulated that the CIP must include risk-based procedures for verifying the identification of a customer that enable the financial institution to form a reasonable belief that it knows the true identity of the customer. The regulations implementing section 326 are commonly referred to as the Customer Identification Program regulations and will be

³The seven federal financial regulators are the Board of Governors of the Federal Reserve Board System (Federal Reserve), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA), Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC). The five SROs included in our review are NASD (formerly the National Association of Securities Dealers) and the New York Stock Exchange (NYSE) for securities broker-dealers and the National Futures Association (NFA), Chicago Mercantile Exchange (CME), and the Chicago Board of Trade (CBOT) for futures commission merchants and introducing brokers. The Internal Revenue Service and the Commissioner of Customs also have delegated authority to investigate and enforce compliance with certain provisions of the BSA regulations.

⁴Section 326 of the PATRIOT Act added a new subsection (l) to 31 U.S.C. §5318.

⁵See Customer Identification Programs for Banks, Savings Associations, Credit Unions and Non-Federally Regulated Banks, 68 Fed. Reg. 25090 (2003); Customer Identification Programs for Broker-Dealers, 68 Fed. Reg. 25113 (2003); Customer Identification Programs for Futures Commission Merchants and Introducing Brokers, 68 Fed. Reg. 25149 (2003); and Customer Identification Programs for Mutual Funds, 68 Fed. Reg. 25131 (2003).

referred to collectively as the “CIP requirement” or the “CIP rule” in this report.⁶

The provisions of section 314 are aimed at encouraging information sharing among financial institutions, their regulators, and law enforcement authorities.⁷ Section 314(a) directed the Secretary to adopt regulations that encourage regulators and law enforcement authorities to share information with financial institutions regarding individuals, entities, and organizations engaged in or reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering activities. Treasury, through FinCEN, adopted final regulations implementing section 314 information sharing procedures in September 2002. The 314(a) regulations set forth the process by which law enforcement agencies provide names and identifying information on suspects to FinCEN.⁸ FinCEN distributes this information to financial institutions across the country and requires that institutions search their accounts to identify any matches. Section 314(b) provides a mechanism to encourage financial institutions, upon notice to the Secretary, to share information with one another regarding individuals, entities or countries suspected of possible terrorist or money laundering activities by providing financial institutions with a safe harbor from liability for disclosing nonpublic personal customer information. Treasury adopted regulations to clarify which financial institutions could share information under section 314(b) and establish the process to be followed by financial institutions that wish to voluntarily share information about their customers and avail themselves of the statutory safe harbor from liability for disclosing such customer information.⁹

⁶Although Section 326 directs Treasury and the federal financial regulators to adopt CIP requirements for all “financial institutions,” which is defined very broadly to encompass a variety of entities, the Secretary may exempt certain financial institutions and accounts from the CIP requirements. To date, Treasury and the federal financial regulators have jointly adopted, and this report is limited to a review of, CIP requirements applicable to (a) banks that are subject to regulation by one of the federal banking regulators, as well as nonfederally insured credit unions, private banks and trust companies; (b) securities broker-dealers; (c) futures commission merchants and introducing brokers; and (d) mutual funds. Accordingly, unless the context otherwise requires, the term “financial institutions” refers to those financial institutions subject to the CIP requirements.

⁷Section 314 is an uncodified provision that appears in the Historical and Statutory Notes to 31 U.S.C. § 5311.

⁸Information Sharing between Federal Law Enforcement Agencies and Financial Institutions, 31 C.F.R. § 103.100 (2002).

⁹Voluntary Information Sharing among Financial Institutions, 31 C.F.R. § 103.110.

To help ensure that the requirements of sections 314 and 326 of the PATRIOT Act are being implemented effectively, you requested that we determine how (1) Treasury (through FinCEN) and the federal financial regulators developed the regulations and addressed challenges, (2) FinCEN and the federal financial regulators informed and educated financial institutions about the new regulations and the challenges such institutions encountered during implementation, (3) the federal financial regulators have updated examination guidance and trained examiners with respect to sections 314 and 326, (4) the federal financial regulators have examined firms for compliance and taken enforcement actions with sections 314 and 326, and (5) the new regulations implementing sections 314 and 326 have affected federal law enforcement investigations and Department of Justice prosecutions of money laundering and terrorist financing cases.

We determined how Treasury (through FinCEN), and the federal financial regulators developed the regulations and overcame challenges by reviewing documentation of the rulemaking process, including comment letters, and interviewing agency officials. To determine how FinCEN and the regulators have educated the industry, we interviewed officials from FinCEN, the federal financial regulators, and SROs about how they have informed and educated the industry and reviewed outreach materials provided to us. We identified implementation challenges encountered by financial institutions through interviews of company officials and industry trade associations representing banks, credit unions, securities broker-dealers, mutual funds, futures commission merchants, and futures introducing brokers. To determine how the regulators and SROs have updated examination guidance and trained examiners, we reviewed draft and final guidance, collected information on examiner training courses and the number of examiners trained for fiscal year 2004, and interviewed officials on their examination guidance and training programs. We also attended an anti-money laundering course for banking examiners. To determine how the regulators and SROs have examined for compliance and taken enforcement actions, we collected data on the number of exams completed from October 1, 2003, through May 31, 2004, and reviewed a sample of 176 examinations from six federal financial regulators and five

SROs.¹⁰ We randomly selected approximately 20 examinations from each regulator and SRO to ensure that the sample was not biased, but our sample should not be interpreted to be representative of all examinations conducted during this time period. We also interviewed officials from FinCEN, the federal financial regulators, and SROs about their examination and enforcement policies and reviewed recent formal enforcement actions. To determine how these new regulations could improve law enforcement investigations, we interviewed officials representing several law enforcement agencies and Department of Justice officials, including supervisory prosecutors who have been involved with money laundering and terrorist financing cases.

We conducted our work between February 2004 and March 2005 in accordance with generally accepted government auditing standards. Additional information on our scope and methodology is discussed in appendix I.

Results in Brief

Treasury and the federal financial regulators had to overcome many challenges to develop regulations implementing the requirements of sections 314 and 326. Developing regulations under section 326 was particularly difficult because Treasury and the federal financial regulators wanted to ensure that CIP procedures were appropriate and consistent across a wide variety of financial institutions that have diverse business models and financial products. In addition, some financial institutions have arrangements with other institutions to process customer transactions. These arrangements and the diversity of business models created challenges for Treasury and the federal financial regulators and concerns among the industry about reasonable levels of accountability for verifying the identity of customers. Developing regulations for section 314 presented practical problems on how to develop a process for information sharing between law enforcement and industry and a process that allows financial institutions to share information with each other. Soon after finalizing regulations, due to feedback from industry that it was overwhelmed by law

¹⁰We selected NASD and NYSE because they oversee the largest percentage of firms in the securities industry and NFA, CBOT, and CME because they oversee the largest number of firms in the futures industry. CFTC was not included in our review of examination guidance and sample of examinations because CFTC conducts oversight reviews of the SROs and at the time of our review, CFTC officials told us that the oversight examinations of SROs they had conducted to date did not focus on compliance with sections 314 and 326.

enforcement information requests, FinCEN suspended the section 314(a) information sharing process and developed a more streamlined approach. Establishing an information sharing process under section 314(b) that defined the parameters of information sharing entitled to the safe harbor protection also presented difficulties because Treasury had to consider how to encourage information sharing while still protecting the customers' right to privacy.

Treasury, the federal financial regulators, and SROs have reached out to the financial industry to help financial institutions understand and comply with the CIP and the section 314 information sharing regulations, though several implementation challenges remain. Treasury, the federal financial regulators, and SROs have distributed written guidance to firms under their jurisdiction, addressed practical, implementation issues at numerous venues such as industry conferences, and clarified the regulations during compliance examinations. These efforts addressed some industry concerns, such as the extent to which firms should verify the identity of existing customers. However, industry officials told us that they continue to experience challenges in implementing CIP procedures and they are concerned about how some of the requirements will be interpreted during examinations. For instance, some industry officials said they remain unsure how examiners will determine that firms have taken sufficient steps to verify the identity of customers and when firms can rely on each other to perform all or some components of a CIP. While industry officials agreed that FinCEN has streamlined and improved the 314(a) information sharing process since the first information request went out in November 2002, the implementation of the 314(a) process has highlighted the tension between law enforcement's duty to protect sensitive information and the need for law enforcement information to help industry better monitor possible financial crimes, including terrorist financing and money laundering. Industry officials continued to be concerned about the limited feedback received from law enforcement despite government efforts to aggregate and supply information to industry on the results of their reporting. Industry officials also said that, although the 314(b) provision has been useful, distinguishing between information that they can and cannot share under the provision is sometimes difficult.

All of the federal financial regulators and SROs in our review issued examination guidance to assess compliance with the CIP requirement and the section 314 information sharing regulations of the PATRIOT Act, and subsequently trained their examiners on the new provisions. Banking regulators jointly issued final examination guidance for section 314 in

October 2003, and the CIP requirement in July 2004. Although banking regulators did not issue guidance for CIP until several months after the regulation took effect, examiners were assessing firms for compliance with the CIP requirement using draft guidance beginning in October 2003. SEC and the securities SROs issued final guidance individually for both provisions. CBOT and CME issued final guidance jointly in February 2004 but were examining firms for compliance with the PATRIOT Act as early as May 2002. NFA issued examination guidance for both provisions by October 2003. Federal financial regulators and SROs continue to update staff on changes to examination procedures using a variety of tools, including teleconferences, monthly or bi-annual staff meetings, interagency bulletins, e-mails, and formal and informal training sessions. By June 2003, all federal financial regulators and SROs had included section 314 regulations and CIP requirements in their examiner training curricula. Both banking and securities regulators used formal training courses that are instructor-led and computer-based. Instruction was also provided internally or by external sources including industry experts and a financial regulators training school. CFTC and the futures SROs provided instructor-led and on-the-job training.

The federal financial regulators and SROs have been examining financial institutions for compliance with CIP and section 314 and taking enforcement actions, but coverage of the provisions in the exams we reviewed varied. In addition, our review revealed some implementation difficulties particularly related to the CIP requirement that could reduce its effectiveness as it applies to high-risk customers and lead to examination inconsistencies. Our review of a sample of 176 examinations conducted from October 1, 2003, through May 31, 2004, showed that CIP procedures were reviewed in 95 percent of the examinations in our sample. While most examinations reviewed whether a financial institution had procedures for meeting the minimum standards for a CIP, fewer examinations (about 56 percent) documented a review of the financial institution's risk-based approach for CIP. Therefore, it was not clear whether all examiners understood that CIP procedures should be more rigorous at financial institutions that have the types of accounts and customers that are at a higher risk for money laundering or terrorist activities as opposed to just meeting the minimum CIP requirements. Also, a few examinations revealed incorrect interpretations by examiners of certain aspects of the CIP requirement that could lead to inconsistencies in how financial institutions understand and apply the CIP requirement. For example, in six examinations, the examiner confused the CIP requirement with other anti-money laundering procedures that require customer identification

information. About 76 percent of the examinations covered section 314(a) provisions in part because some regulators were still developing examination procedures, and about 55 percent of the examinations covered section 314(b) in part because the sharing of information pursuant to this provision is voluntary. The extent of coverage in the examinations of the various aspects of the CIP requirement and section 314 provisions may have also varied because (1) examiners used different approaches to document their work and therefore may have limited our ability to fully know what was reviewed and (2) the examinations we reviewed were conducted during early implementation. Because the regulations were new and many deficiencies were technical mistakes, federal financial regulators and SROs mostly took informal actions to address deficiencies or violations of CIP and section 314.

Officials from the Department of Justice and other law enforcement agencies told us that section 314(a) and the CIP requirement have assisted in the investigation of money laundering and terrorist financing cases. Many of the law enforcement officials we interviewed said that the 314(a) information sharing process has improved coordination between law enforcement agencies and financial institutions and has increased the speed and efficiency of investigations. For example, a senior official from the Federal Bureau of Investigation (FBI) described how a 314(a) information request led to the identification of additional accounts associated with a suspect across 23 states and 45 financial institutions. Prior to learning this new information, the FBI was aware of only four accounts. The law enforcement officials we spoke with also believed that the section 314(a) process facilitates the flow of information between law enforcement and financial institutions because the process connects law enforcement with approximately 20,000 financial institutions, and the 314(a) information requests include points of contact with law enforcement. Some law enforcement officials told us that CIP has also been useful because financial institutions have more information about their customers. Therefore, law enforcement agencies obtain more consistent and useful customer information when issuing grand jury subpoenas and 314(a) requests. Justice officials, including those from U.S. Attorneys offices who have prosecuted money laundering and terrorist financing cases, told us that decisions about whether to pursue an investigation and prosecute money laundering cases depend on a myriad of factors and are made on a case-by-case basis. Therefore, although they believe that the section 314(a) and CIP requirements are important to law enforcement and provide valuable information to investigations, they did not believe that these new tools will necessarily result in an increase in the

number of money laundering and terrorist cases that they choose to prosecute.

In this report, we make recommendations to Treasury, through FinCEN, to work with the federal financial regulators to develop guidance that should address industry concerns about some of the CIP requirements and improve examinations of CIPs. In responding to our draft report, Treasury agreed that additional guidance would improve implementation of these regulations.

Background

Money laundering is the process used to transform monetary proceeds derived from criminal activities into funds and assets that appear to have come from legitimate sources. Terrorist financing is generally characterized by different motives than money laundering and the funds involved often originate from legitimate sources. However, the techniques for hiding the movement of funds intended to be used to finance terrorist activity—techniques to obscure the origin of funds and the ultimate destination—are often similar to those used to launder money. Therefore, Treasury, federal law enforcement agencies, and the federal financial regulators often employ similar approaches and techniques in trying to detect and prevent both money laundering and terrorist financing.

Following the September 11 terrorist attacks, Congress passed the USA PATRIOT Act, which was enacted on October 26, 2001. Title III of the PATRIOT Act amended the BSA. The BSA was enacted by Congress in 1970 and requires that financial institutions file reports and maintain records with respect to certain transactions in currency and monetary instruments that are determined to have a high degree of usefulness in criminal, tax, or regulatory investigations and, as amended by the PATRIOT Act, these records and reports also have a high degree of usefulness in the conduct of intelligence or counterintelligence activities.¹¹ As a result, the BSA helps to provide a paper trail of the activities of money launderers for law enforcement officials in pursuit of criminal activities. Congress has amended the BSA several times to give the U.S. government a wider variety of regulatory tools to combat money laundering. In addition to requiring

¹¹31 U.S.C. § 5311. The regulations adopted by Treasury implementing the BSA are codified at Part 103 of Title 31 of the Code of Federal Regulations (BSA Regulations). As used in this report, and unless otherwise specified, BSA collectively refers to the statutory provisions and the BSA Regulations.

regulations for information sharing and customer identification programs, Title III of the PATRIOT Act expands Treasury's authority to regulate the activities of U.S. financial institutions and requires a wide variety of types of financial institutions to maintain anti-money laundering programs.

Agencies under the Departments of the Treasury, Justice, and Homeland Security are to coordinate with each other and with federal financial regulators in combating money laundering and terrorist financing. Within Treasury, FinCEN, under delegated authority from the Secretary of the Treasury, is the administrator for the BSA and supports law enforcement agencies by collecting, analyzing, and coordinating financial intelligence information to combat money laundering. As a bureau of Treasury, FinCEN clears all BSA regulations through Treasury. In August 2004, FinCEN created an Office of Compliance to oversee and work with the federal financial regulators on BSA examination and compliance matters. FinCEN signed a Memorandum of Understanding (MOU) with the banking regulators in September 2004 that laid out procedures for the exchange of certain BSA information. The MOU requires that the federal banking regulators provide information on examination policies and procedures and on significant BSA violations or deficiencies that have occurred at the financial institutions they supervise, including relevant portions of examination reports and information on follow-up and resolution. FinCEN will also provide information to the banking regulators, including information on FinCEN enforcement actions and analytical products that will identify various patterns and trends in BSA compliance. FinCEN has been working on similar MOUs with SEC and CFTC; however, as of March 25, 2005, no effective dates have been set for either of them.

Department of Justice components involved in efforts to combat money laundering and terrorist financing include the Criminal Division's Asset Forfeiture and Money Laundering Section and Counterterrorism Section, the FBI, the Bureau of Alcohol, Firearms, and Explosives, the Drug Enforcement Administration, and the Executive Office for U.S. Attorneys (EOUSA) and U.S. Attorneys Offices. The Department of Homeland Security's Bureau of Immigration and Customs Enforcement (ICE) also investigates cases involving money laundering and terrorist activities.

The federal financial regulators who oversee financial institutions and examine them for compliance with anti-money laundering laws and regulations include the federal banking regulators—the Federal Reserve, OCC, OTS, FDIC, and NCUA—and SEC, which regulates the securities markets, and the CFTC, which regulates commodity futures and options

markets. Because the U.S. securities and futures markets are regulated through a combination of self-regulation (subject to federal oversight) and direct federal regulation, the SROs also oversee compliance with anti-money laundering laws and regulations. Two of the SROs—NASD and NYSE—oversee registered broker-dealers. NFA oversees futures commission merchants and introducing brokers in commodities.¹² In addition to NFA, a number of the futures commission merchants are overseen by futures exchanges, including the New York Mercantile Exchange, CME, and CBOT.

Developing Regulations for CIP and Section 314 That Applied to a Wide Range of Financial Institutions Was Difficult and Complex

Treasury and the federal financial regulators encountered numerous challenges as they developed regulations to implement sections 314 and 326. Key challenges related to implementing section 326 included developing regulations that could be applied consistently across a financial industry that has diverse business models, customer relationships, and financial products. In addition, many financial institutions have arrangements with other institutions to process customer transactions. These arrangements and the need to build in a risk-based approach to customer identification created concerns among the regulators and industry about reasonable levels of accountability for verifying the identity of customers. Developing regulations for section 314 presented practical problems on how to develop a process for information sharing between law enforcement and industry and a process that allows financial institutions to share information with each other.

¹²NFA also oversees commodity trading advisors and commodity pool operators; although the Secretary of the Treasury has deferred application of the anti-money laundering requirements to these financial institutions for an unspecified period, Treasury has proposed rules that would require commodity trading advisors and commodity pools to implement anti-money laundering programs. See 68 Fed. Reg. 23640 (May 5, 2003) (commodity trading advisors); 67 Fed. Reg. 60617 (September 26, 2002) (unregistered investment companies, including commodity pools). Futures commission merchants can be individuals, associations, partnerships, corporations, and trusts that solicit or accept orders for the purchase or sale of any commodity for future delivery on or subject to the rules of any exchange and that accept payment from or extend credit to those whose orders are accepted. An introducing broker for commodities is a person engaged in soliciting or accepting orders for the purchase or sale of any commodity for future delivery on an exchange who does not accept any money, securities or property to margin, guarantee, or secure any trades or contracts that result there from.

Development of the CIP Requirement Highlighted Difficulties in Applying Requirements Consistently to a Wide Range of Financial Products and Businesses

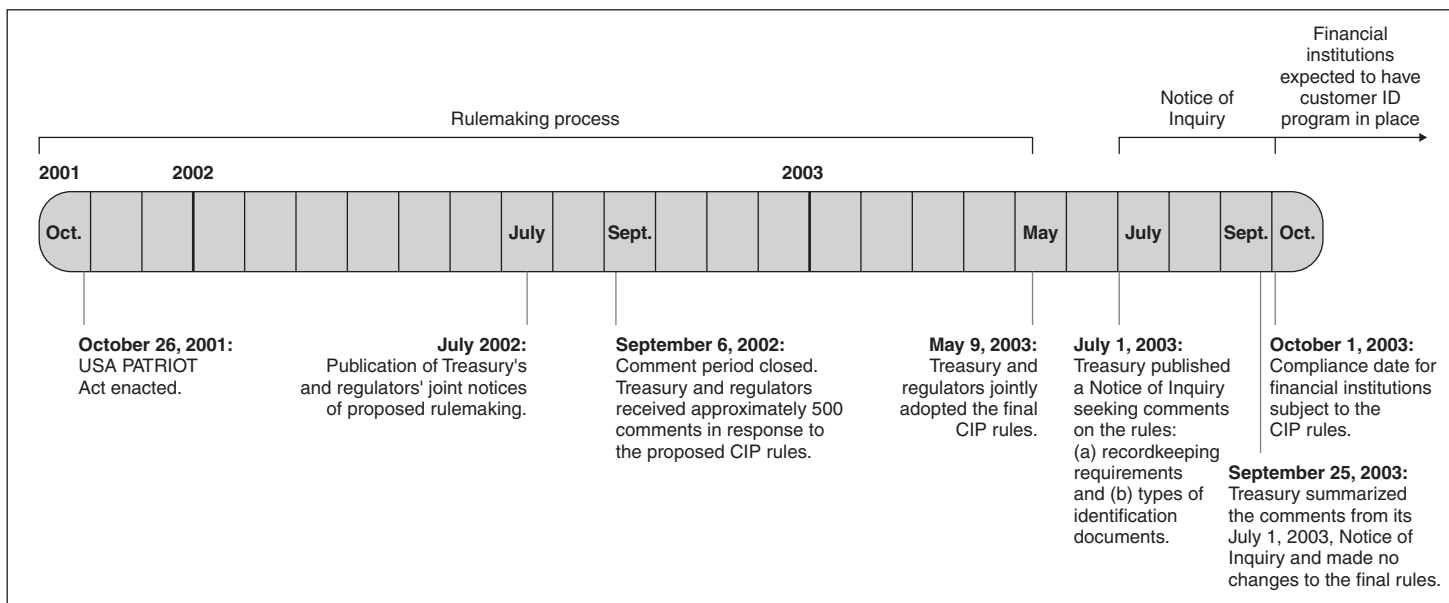
Treasury and the federal financial regulators had to resolve several issues through an interagency process when developing the regulations for CIP, such as defining “customer” and “account” for the purposes of the regulations and determining how much flexibility to give firms in verifying the identity of customers. Because the regulations for CIP would apply to a diverse financial industry, FinCEN and the regulators formed a working group and gathered information from industry officials about their different business models and customer relationships. According to FinCEN officials, the interagency process employed to issue joint regulations was the first that included Treasury and the seven federal financial regulators. Specifically, Treasury and the five banking regulators (FDIC, Federal Reserve, NCUA, OCC, and OTS) jointly adopted a CIP rule covering banks, thrifts, and credit unions.¹³ Treasury and SEC jointly adopted separate rules for broker-dealers and mutual funds.¹⁴ Treasury and CFTC jointly adopted a rule for futures commission merchants and introducing brokers.¹⁵ As shown in figure 1, the rulemaking process took over a year and a half to complete.

¹³31 C.F.R. § 103.121. Although the substantive provisions of the four joint CIP rules are codified in 31 C.F.R. part 103, subpart I – Anti-Money Laundering Programs, each of the federal financial regulators concurrently published a provision in its own regulations to cross-reference the final rules in order to clarify the applicability of the final rules to the financial institutions subject to their respective jurisdictions.

¹⁴31 C.F.R. §§ 103.122 and 103.131.

¹⁵31 C.F.R. § 103.123.

Figure 1: Key Dates in the Rulemaking Process for CIP






Source: GAO.

Following the issuance of the joint notices of proposed rulemaking in July 2002, Treasury and the federal financial regulators collectively received approximately 500 comments, many of which expressed concerns about the types of accounts and customers that should be subject to CIP. For instance, some comments questioned whether an account established as part of an employee benefit plan should be subject to CIP regulations, the extent to which the risk-based approach should be used, and the need for Treasury and the federal financial regulators to be more specific about the methods of verification. Other comments proposed that the entire process be risk-based without any minimum requirements. Some comments also addressed how financial institutions could rely on or share responsibility with another institution for verifying the identity of a shared customer account. This reliance aspect is important for some types of financial institutions that have securities and futures products. For example, in the securities industry, many brokers interact with customers (introducing brokers) but rely on another broker for clearance, settlement, and custody purposes (clearing firms). Typically under this arrangement the introducing broker interacts with the customer by taking orders and making recommendations and the clearing firm holds the customer assets. Treasury and the regulators also considered how financial institutions

could verify customer identities for customers who open accounts by mail, by phone, or over the Internet.

Treasury and the federal financial regulators ultimately established minimum identification requirements and mandated that financial institutions develop risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The verification procedures included documentary and nondocumentary methods to cover the variety of approaches customers use to open accounts. The final rules published on May 9, 2003, provide a framework with minimum standards for identifying customers, while allowing financial institutions flexibility to design and implement CIPs according to risk-based procedures for verifying identity based on their business lines, types of customers, and methods of opening accounts. Figure 2 illustrates requirements for identification and verification procedures.

Figure 2: Requirements for Customer Identification and Verification Procedures

					Factors considered for a risk-based approach			
					<input type="checkbox"/> Type of account		<input type="checkbox"/> Methods of opening account	
Minimum information requirements			Verification methods		Additional verification methods			
			Documentary		Nondocumentary			
Individual <ul style="list-style-type: none"> • Name • Date of birth • Physical address • ID number <ul style="list-style-type: none"> • U.S. person (taxpayer identification number) • Non-U.S. person (taxpayer identification number or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard) 			Unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport 		May include contacting a customer; comparing the customer information with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement		The CIP must address situations where, based on the institution's risk assessment of a new account opened by a customer that is not an individual, the institution will obtain information about individuals with authority or control over such account, including signatories, in order to verify the customer's identity. This verification method applies only when the institution cannot verify the customer's true identity using the other verification methods.	
Legal entity <ul style="list-style-type: none"> • Name • Physical address, such as principal place of business • ID number <ul style="list-style-type: none"> • U.S. entity (taxpayer identification number) • Non-U.S. entity (the financial institution must request alternative government-issued documentation certifying the existence of the business or enterprise if the entity does not have an identification number) 			Documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument 					

Source: GAO analysis of regulations for CIP.

In addition to establishing minimum identification standards and a risk-based approach for verification procedures, the final rule requires that financial institutions develop CIPs that include procedures for (1) making and maintaining a record of information required to be obtained from the customer at the time the account is opened and retaining the information

for five years after the date the account is closed,¹⁶ (2) providing notice to the customer that their identity will be verified, and (3) determining whether a person appears on any list designated by Treasury (in consultation with the federal financial regulators) as a federal government list of known or suspected terrorists or terrorist organizations that must be checked by financial institutions as part of the CIP requirement. Treasury has not designated a list for the CIP requirement at this time.

The final rule also allows financial institutions to rely on another financial institution to perform any procedures of its own CIP for customers that the two financial institutions share provided that, among other requirements, the financial institution that is being relied on enter into a contract certifying annually to the relying financial institution that it has implemented its own anti-money laundering program and that it will perform the specified requirements of the relying financial institution's CIP. The rule also requires that the financial institution being relied on is regulated by a federal functional regulator. The final rules stated that financial institutions were expected to be in compliance with the final rules no later than October 1, 2003.

Treasury issued a Notice of Inquiry in July 2003 (see fig. 1) approximately 2 months after the final CIP rules had been adopted, soliciting additional comments about two aspects of the final CIP rules that concerned some interested parties, including members of Congress and law enforcement officials. The Notice of Inquiry sought additional comments on (1) whether and under what circumstances financial institutions should be required to retain photocopies of identification documents relied on to verify customer identity and (2) whether there are situations when the regulations should preclude reliance on certain forms of foreign government-issued identification to verify customer identity. Treasury received over 34,000 comments in response to the Notice of Inquiry from a wide variety of individuals and entities, including members of Congress, the Department of Justice, the financial services industry, advocacy groups, and interested citizens.

Treasury did not make any changes to the final CIP rules for two reasons. First, it concluded that requiring photocopies in all cases is not consistent with the risk-based approach for CIP. In its official disposition of comments

¹⁶Other records of information, such as documents used to verify a customer's identity, obtained pursuant to a CIP must be retained for five years after the record is made.

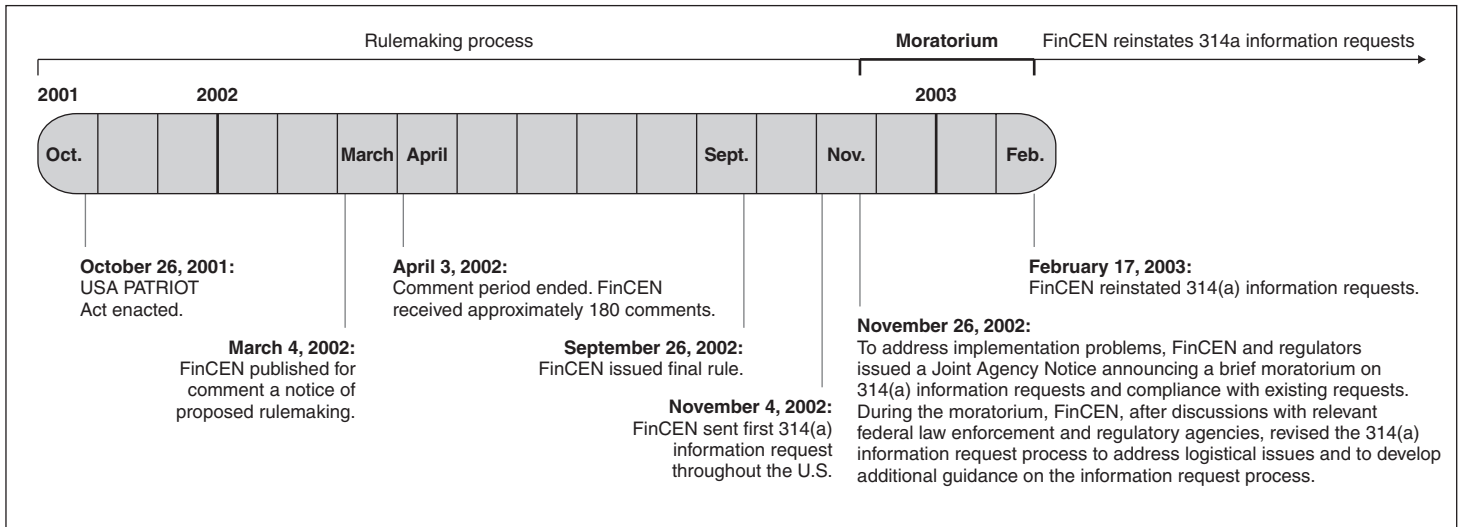
to the notice, Treasury said that the decision to make photocopies should be at the discretion of the financial institution rather than an across-the-board requirement. Second, Treasury decided that specifying individual types of documents that cannot be relied upon to verify customer identities did not make sense from a regulatory perspective because the relative security and reliability of various identification documents that are available is constantly changing. The comments received in response to the Notice of Inquiry primarily related to encouraging Treasury to take an official position on whether the Mexican consular identification document, the *Matricula Consular* is a reliable document for verifying identification.¹⁷ Treasury concluded that because the relative security and reliability of identification documents are constantly changing, any list of unacceptable documents would quickly become outdated and may provide financial institutions with an unwarranted sense of security concerning documents that do not appear on such a list. Therefore, Treasury decided not to prescribe a specific list of documents that are acceptable or not acceptable in the regulation, but rather committed to providing financial institutions with information relating to the security and reliability of identification cards.

Developing Section 314 Regulations Required Balancing the Needs of Law Enforcement and Industry

When developing section 314 regulations, Treasury (through FinCEN) had to determine the extent to which financial institutions should share information about customers with law enforcement officials and with each other. Treasury adopted final regulations in September 2002. Figure 3 shows the key dates in the rulemaking process for section 314.

¹⁷In a 2004 report, we found that consular identification cards are issued by some governments to help identify their citizens living in a foreign country, but that federal agencies hold different and, in some cases, conflicting views on the usage and acceptance of these cards and no executive branch guidance is yet available. See U.S. Government Accountability Office, *Border Security: Consular Identification Cards Accepted within United States, but Consistent Federal Guidance Needed*, [GAO-04-881](#) (Washington, D.C.: Aug. 24, 2004).

Figure 3: Key Dates of the Rulemaking Process for Section 314



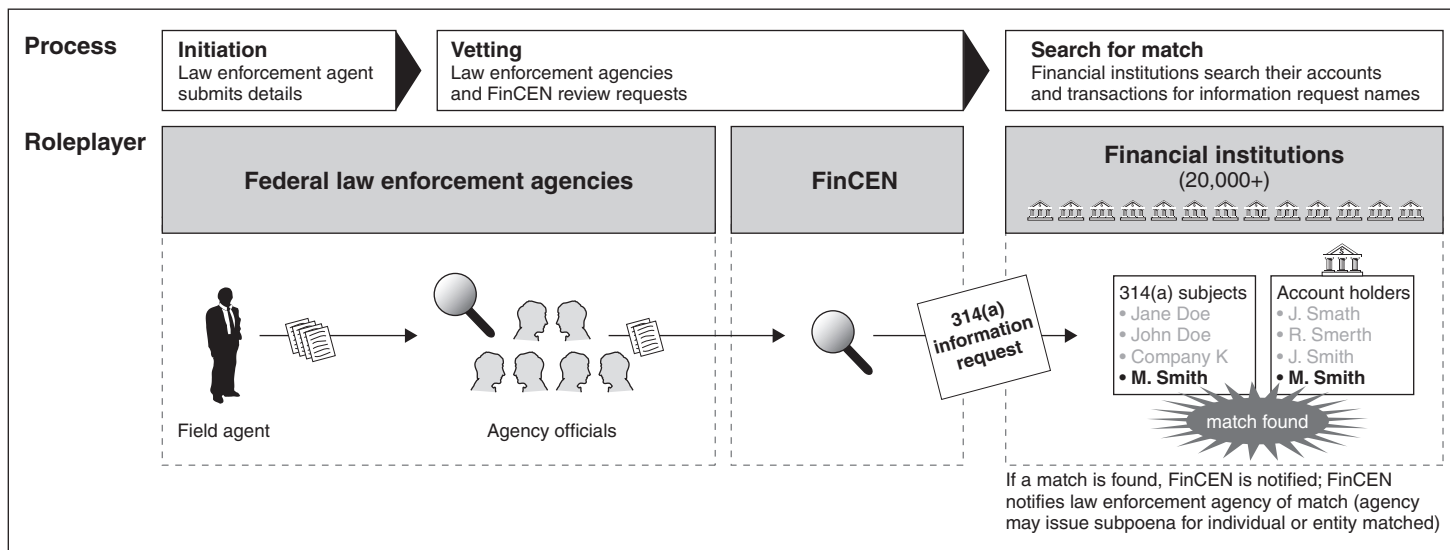
Source: GAO.

For section 314(a), FinCEN implemented a process in which law enforcement agencies provide information on potential suspects to FinCEN. FinCEN distributes these 314(a) information requests across the country to financial institutions that are required to search their accounts and transactions to identify any matches.

The process was temporarily suspended in November 2002, based on feedback from financial institutions that they were overwhelmed or confused by the process. Some institutions did not know what to do with the information requests, while others were not sure which accounts or transactions to search. Following consultations with law enforcement and the federal financial regulators to streamline the process, FinCEN resumed 314(a) information requests in February 2003. FinCEN and industry officials agreed that, since the moratorium, FinCEN has implemented a more streamlined process that has improved the clarity and efficiency of 314(a) information requests. Officials from FinCEN and law enforcement agencies have also established procedures to vet requests sent by law enforcement agencies to ensure that they are related to terrorist or significant money laundering activities. (See fig. 4.) Before putting a name on the information request list, FinCEN officials said that they follow up with the requesting law enforcement agent to obtain more information to determine whether the case merits the use of the 314(a) process and to

verify that the agent will be available to respond to any financial institution that finds a match when the request goes out. FinCEN also sends each law enforcement requester a feedback form on the usefulness of the information obtained. For example, the feedback form asks if law enforcement officials served grand jury subpoenas based on the information obtained from the 314(a) process. In addition, law enforcement officials said that they have taken steps to caution agents against overusing the 314(a) process, and that the 314(a) process is not meant to replace the need for a subpoena or more rigorous investigation methods.

Figure 4: The 314(a) Information Sharing Process after the Moratorium



Source: GAO.

FinCEN sends out the 314(a) information request list every 2 weeks. The information requests include suspects related to terrorist cases and significant money laundering investigations. FinCEN tries to limit the number of subjects on the bi-weekly information request. The request contains as much identifying information as possible, such as dates of birth, social security numbers, and addresses as well as aliases so the

number of records that are to be searched for can be extensive.¹⁸ Financial institutions have 2 weeks to respond. Urgent requests can also be distributed with shorter turnaround time when deemed necessary.

The rulemaking process for section 314(b) addressed the need to encourage information sharing among financial institutions while still protecting customers' right to privacy and established a mechanism for financial institutions to satisfy the statutory notice requirement. Section 314(b) of the PATRIOT Act allows financial institutions, upon providing notice to Treasury, to share information regarding individuals, entities, and countries suspected of possible terrorist or money laundering activities.¹⁹ The final rule requires that to be protected by the safe harbor from liability for sharing information pursuant to section 314(b), financial institutions must comply with the procedures prescribed by the rule, including providing notice annually to FinCEN of their intent to share information with other institutions. The rule also requires that prior to sharing information, a financial institution must verify that the financial institution with which information will be shared has also filed a notice with FinCEN. FinCEN determines that the notice requirement sufficiently reminds financial institutions of their need to safeguard information that is obtained using section 314(b).

¹⁸Effective March 1, 2005, FinCEN implemented a Web-based USA PATRIOT Act Section 314(a) Secure Information Sharing System. The new system allows for a streamlined, secure Web-enabled delivery of 314(a) information to financial institutions and more efficient reporting of matches back to FinCEN.

¹⁹Although there is no statutory requirement that regulations implementing section 314(b) be adopted, FinCEN determined that such rules were needed to specify the kinds of institutions that would be permitted to share information and to clarify how such financial institutions could provide the requisite notice of their intent to share information. The rules adopted under section 314(b) apply to financial institutions that are required to establish and maintain an anti-money laundering program, or are treated as having satisfied the requirements of Treasury's anti-money laundering program regulations. See 31 C.F.R. § 103.110.

Treasury and the Federal Financial Regulators Have Reached Out to the Financial Industry to Assist It in Implementing CIP and Section 314 Rules, but Industry Concerns Remain

Treasury and the federal financial regulators have taken several steps to help the financial industry understand and comply with the CIP and 314 information sharing regulations; however, the need for agency coordination has slowed the issuance of additional guidance. Industry officials said that although the government's guidance has been helpful, it does not completely address their questions and compliance concerns particularly related to the CIP rule. The implementation of the 314(a) information sharing process has highlighted the tension between law enforcement officials' duty to protect sensitive information and the need for information from law enforcement to help industry monitor, identify, and report possible financial crimes, including terrorist financing and money laundering. Finally, industry officials said that they appreciate the safe harbor provided by 314(b), but some officials said distinguishing possible money laundering and terrorist activities from other types of financial crimes not covered by section 314(b), such as fraud, has been difficult.

Treasury and the Regulators Have Assisted Industry in Implementing CIP and Section 314 Requirements, but Interagency Coordination Has Slowed Issuance of Additional Guidance

Treasury and the federal financial regulators have sought to educate the financial community to help it understand the new requirements, but the need for interagency coordination has slowed regulators' issuance of additional guidance. Regulators and SROs used established, formal channels (such as Web site postings and existing regulatory memorandums distribution channels) to distribute guidance to firms describing the regulations, clarifying when the regulations would become effective, and offering advice about implementation. Officials from the regulatory agencies and SROs also informed firms of the regulations and addressed practical issues during numerous industry-related conferences, conference calls, and training sessions. Moreover, agency officials said that during compliance exams conducted before and soon after the regulations became effective, examiners clarified particular aspects and helped firms establish compliant programs.

Treasury and the federal financial regulators have provided specific guidance related to the CIP rule and section 314 in the form of responses to "frequently asked questions" or "FAQs." In August and October 2003, Treasury and SEC issued limited FAQ guidance related to mutual funds and broker-dealers, respectively. In January 2004, Treasury and the banking regulators jointly issued FAQ guidance that addressed several issues related to CIP. Among other topics, the answers clarified the definitions of a customer and an account in different situations and discussed how firms should apply the rules to existing customers. In July 2004, Treasury and

CFTC issued FAQ guidance concerning CIP that was similar to the banking regulators' guidance.

FinCEN issued FAQs for the 314 information sharing regulations in February 2003. These FAQs were initially posted on FinCEN's public Web site but, according to FinCEN officials, they were removed due to law enforcement concerns that this guidance could give criminals an advantage. FinCEN officials said they have now posted these FAQs to its secure Web site that financial institutions access to obtain the 314(a) information requests and will send the FAQs to a financial institution upon request.

According to FinCEN, because of the joint nature of the CIP rules, all of the affected regulators and FinCEN must coordinate when issuing guidance to assure consistency in the implementation of the regulations. Such coordination has slowed the issuance of further guidance. Similar to the challenges they encountered in the rulemaking process, the financial regulators and FinCEN face continuing challenges in developing guidance that applies to diverse types of financial products and businesses. FinCEN and the federal financial regulators began developing a second series of CIP FAQs pertaining primarily to banks in early 2004. Some officials told us that this guidance has taken longer to finalize because of difficulties reaching agreements on which questions to address and how to answer them. FinCEN officials told us that although some of the officials had signed off on the draft FAQs, agreement was not reached among two of the regulators on one outstanding question until February 2005. FinCEN officials told us that, although these are questions pertaining to CIPs, some questions have broader policy implications for the affected agencies. FinCEN released the draft for internal approval by the financial regulators on March 25, 2005, and the final CIP FAQs were jointly issued by Treasury, FinCEN, and the banking regulators on April 28, 2005. Officials from CFTC and FinCEN told us that they hoped guidance in the form of an FAQ addressing the CIP issue related to customers of executing and carrying brokers would be released soon, but it has also taken some time to finalize the guidance. SEC officials told us that they have been waiting for the second set of banking FAQs and will then adapt the first and second set of CIP FAQs for securities firms.

The industry officials we spoke with largely agreed that the regulators have provided valuable information and services helping them to understand the regulations. Some officials lauded the time and effort regulators have taken

to inform firms of the new regulations and answer difficult, practical questions.

Industry Officials Believe That More Guidance from FinCEN and Financial Regulators Would Help Address Some CIP Implementation Challenges

Industry officials we met with said that while regulators' guidance has been helpful, it does not address all of their questions and concerns, thus making it difficult for them to know if they are in full compliance with the requirements. Industry officials said that although their institutions had customer identification procedures in place prior to the PATRIOT Act, they revised their forms, processes, and systems to meet the minimum CIP requirements. Many industry officials said that CIP regulations have challenged them to organize and document their identification procedures, create new forms and processes to notify customers of the new procedures, and reconfigure systems in order to store information required by the regulations for the specified period. Industry officials also said that implementing CIP has improved the consistency of customer identification procedures across different business lines in their own institutions and should improve consistency across the various financial sectors.

CIP FAQs that FinCEN and the federal financial regulators issued for bank, securities, and futures firms in 2003 and 2004 responded to several of the industry's implementation concerns. For example, the FAQs for banks discussed two issues banks raised during the public comment period in the rulemaking process—(1) the extent to which banks should verify existing customers and (2) how banks may identify customers using nondocumentary sources of identification information. The one CIP FAQ for securities firms clarified when an intermediary will be deemed the customer for purposes of the CIP rule when opening a domestic omnibus securities account to execute transactions for the intermediary customers.

Despite the guidance, industry officials remain concerned about some challenges they raised during the comment period and have additional concerns. For example, industry officials said they are still uncertain how examiners determine that firms have taken appropriate steps to verify the identity of customers when the CIP regulations allow firms to take a risk-based approach and give them the flexibility to tailor their procedures for verifying customers' identities according to their location, customers, and products. Industry officials believe that they and their examiners may reasonably disagree on the risks posed by certain customers and subsequently disagree about when to take extra steps to verify the identity of the customers. The officials expressed concern that examiners will sanction firms who differed with them, despite the fact that the firms

followed what they believed were reasonable steps to determine the risk of the customers and subsequently took reasonable steps to verify their identity. For example, one industry representative told us that in a recent exam an examiner questioned the firm's designation of high-risk countries--the firm planned to take more stringent steps to verify the identity of customers depending on the risk ranking of high-risk countries. According to the industry official, the examiner thought that two of the countries on the risk matrix should have been placed in a higher risk category but did not provide a basis for believing that certain countries should be higher on the firm's risk ranking.

Some industry officials also said that they were unsure how examiners expected them to verify the identity of institutions and people when reliable identification information is unavailable, such as for people from countries where sources of identification may not be reliable. CIP rules require that financial institutions collect a government identification number for corporations as well as individuals. Some industry officials said that a foreign government identification number for institutions or corporations can be very difficult to verify and therefore the collection of the identification number is virtually worthless. Also, one of the documentary methods for verifying the identity of a corporation is to obtain the articles of incorporation, but these documents can also be difficult to use to verify identities for foreign entities. Some securities industry officials told us that foreign incorporation documents are difficult to obtain and sometimes impossible because the country does not make this information available to the public. Similarly, officials from mutual fund firms expressed uncertainty concerning how examiners will assess their practices for verifying the identity of some customers processed online or over the telephone. The officials explained that they often use credit reports and other nondocumentary sources to verify these types of customers, and such sources are not always available for some customers, such as young customers or some senior customers.

Additionally, some industry officials expressed uncertainty about the reliance provision of the CIP rule. Specifically, industry officials said that they did not know the scope of a reasonable reliance agreement and which firm is liable for mistakes. Even after regulators issued guidance on the reliance provision in the first series of CIP FAQs, some industry officials said that they remain uncertain about the scope of reasonable reliance agreements in some instances. Industry officials in the futures industry told us that they hope that the federal government will provide guidance on how the CIP requirement affects the relationship between executing brokers

and carrying brokers in “give up” relationships.²⁰ CFTC and NFA officials said that the regulations suggest that for an executing broker to invoke the reliance provision in give-up transactions, carrying brokers must certify that they have verified the identity of each customer whose trades are given up to the carrying broker, thus requiring numerous verifications, which could overwhelm the daily operations of the firms with CIP requirements. In February and March 2005, CFTC and FinCEN officials told us that they were working to issue additional guidance concerning these give-up relationships and they hoped it would be issued shortly. In addition, some industry officials said that they avoid relying on other firms because they did not know how examiners would determine which firm will be responsible for mistakes. During the rulemaking process, officials from the securities sector expressed this same concern. Some industry officials told us that examiners did not fully understand the reliance provision. The securities industry officials told us that the reliance provision was meant to ensure that the CIP requirement did not result in duplicative efforts. Because of these concerns, some firms may not take advantage of the provision.

Industry Officials Faced Some Implementation Challenges and Question Whether the 314(a) Information Sharing Process Improves Communication with Law Enforcement

The implementation of the 314(a) information sharing process has created some practical challenges and highlighted the tension between law enforcement officials’ duty to protect sensitive information and industry’s need for information useful in identifying and reporting financial crimes, including terrorist financing and money laundering. One challenge industry officials said they faced was their inability to simultaneously search the multiple customer databases they are required to search, which forces them to search numerous databases individually. Some industry officials told us that they have dedicated significant staff hours to conduct the searches, developed search programs specifically for 314(a) information requests, and hired third-party vendors to conduct the searches.

²⁰According to CFTC officials, the CIP rule (and other CFTC rules) place responsibility for customer identification procedures on futures commission merchants that are carrying brokers because they deal directly with customers and have the systems and procedures for identifying customers. However, a customer may elect to use one or more executing futures commission merchants to place a given trade for a number of reasons (e.g., the customer’s carrying broker may not be a member of the particular exchange on which the contract in question is listed for trading). In this situation, the customer would need another futures commission merchant—the executing broker—to conduct the trade (i.e., the executing broker “gives up” the trade). Executing brokers have not historically had to identify these types of customers.

Despite the attempts to lessen the burden of the 314(a) process, some industry officials said that they have been disappointed with how federal law enforcement agencies appear to be using the process. Industry officials said that they expected law enforcement officials to request information only for select, serious threats and primarily terrorist-related activities; however, they questioned the significance of some of the information requests they have received because requesting law enforcement agents have not followed up matches by sending subpoena requests or returning telephone calls concerning the matches. FinCEN and law enforcement agency officials responded that they continue to refine the process for vetting requests and preventing agents from overburdening financial institutions with unnecessary requests.

Also, some industry officials asked why law enforcement officials could not provide more information about cases involving their institutions, how to treat particular suspicious customers, and profiles of terrorists and other criminals. The industry officials said that such information would help them to recognize and report a potential criminal or terrorist and enable them to update their criteria for assessing the risk of individual customers, thus strengthening due diligence systems and improving their contributions to law enforcement officials' anti-money laundering and anti-terrorism efforts. Law enforcement and FinCEN officials said that although they greatly appreciate the information provided by firms via the 314(a) process, providing feedback to firms on particular cases can be a challenge, particularly when cases involve sensitive information. In August 2004, the FBI created a list of terrorist financing indicators to assist financial institutions in identifying and reporting suspicious activity that may relate to terrorism. FinCEN forwarded this information to financial institutions through the 314(a) distribution channels. Consistent with the statements of the law enforcement officials we spoke with, the 9-11 Commission praised the benefits of the section 314(a) information sharing process, but also expressed concerns about the extent to which law enforcement should share sensitive law enforcement or intelligence information. The 9-11 Commission noted that providing financial institutions with information concerning ongoing investigations opens up the possibility that the institutions may leak sensitive information, compromise investigations, or violate the privacy rights of suspects.

In response to the industry's request for more information concerning the value of the 314(a) process, FinCEN periodically publishes 314(a) fact sheets. These fact sheets provide industry with summary data on 314(a) requests over a specific time period, including the law enforcement

agencies making requests and the number of search warrants, grand jury subpoenas, and indictments attributable to information firms provide through the 314(a) process. Regulators, industry officials, and law enforcement officials also jointly publish semiannual Suspicious Activity Report (SAR) Activity Reviews, which provide information on trends and patterns in financial crimes and how industry's contributions through reporting suspicious activity and responding to 314(a) requests have helped investigations. Furthermore, as stated in its Fiscal Year 2006-2008 Strategic Plan, released in February 2005, FinCEN plans to seek faster and more efficient technical channels for dialog between government and the financial industry. For example, FinCEN officials told us that they hope to use FinCEN's new secure information sharing system to provide financial institutions additional feedback information.

Industry Officials Expressed Some Confusion about Types of Suspicious Activity That Can Be Shared under Section 314(b)

Although industry officials said section 314(b) is a helpful tool and has enabled them to share information in a new way, some officials said it is not always easy to determine if the suspicious activity is money laundering or terrorist activity or other financial crimes. As noted earlier, section 314(b) of the PATRIOT Act provides a safe harbor for financial institutions to protect them from liability for sharing information only if it relates to individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities. Some industry officials stated that sometimes it is difficult to distinguish fraudulent activity from possible money laundering, thus making it hard to determine if a firm can share information about that activity with other firms participating in the 314(b) network. As a consequence, some financial institutions may be reluctant to use the 314(b) process.

On the positive side, industry officials who had used the process said that the 314(b) provision has allowed firms to share useful information regarding potential money laundering or terrorist activities with other institutions that they previously had little or no interaction with. The officials said that such sharing has helped them efficiently collect otherwise unattainable information about customers, enabling their firms to practice better due diligence. Furthermore, some officials from the banking industry said the 314(b) safe harbor provision has encouraged them to give and receive information that uncovers diverse criminal activities because money laundering is a predicate to a wide variety of crimes.

Financial Regulators and SROs Have Updated Examination Guidance and Trained Examiners to Evaluate Compliance with CIP and Section 314

Since February 1 and October 1, 2003—when financial institutions were to be in compliance with regulations for sections 314 and CIP of the PATRIOT Act, respectively—banking, securities, and futures regulators and SROs issued examination guidance and trained examiners to assess firms for compliance with both provisions. The five banking regulators jointly issued guidance for CIP and section 314. The SEC and the securities SROs we reviewed issued final guidance for both provisions individually, and the futures SROs we reviewed issued final guidance jointly in February 2004 through the Joint Audit Committee—a consortium of futures exchanges. NFA updated and issued its guidance by October 2003 for both provisions. All federal financial regulators and SROs continue to update staff on changes to examination procedures and have trained examiners to assess firms for compliance with CIP and section 314.

All Financial Regulators and SROs Have Issued Final Guidance and Procedures for CIP and Section 314 and Used a Variety of Methods to Communicate Changes to Their Staff

The banking regulators jointly issued guidance and procedures for section 314 on October 20, 2003, and for CIP on July 28, 2004. Although banking regulators did not issue final examination guidance for CIPs until several months after the regulations took effect, examiners were assessing firms' CIPs using draft or interim guidance beginning in October 2003. SEC issued final guidance and procedures for broker-dealers in September 2003 and April 2002 for mutual funds.²¹ SEC's guidance for mutual fund examination does not address examination for compliance with section 314(a) requests to mutual funds. SEC officials told us that FinCEN is currently not including mutual funds in the 314(a) process.²² Also, SEC officials said that

²¹According to the timeline presented in figure 1 in this report, SEC's mutual fund exam guidance was updated to include CIP before Treasury issued the notice of proposed rulemaking for section 326 in July 2002. When we asked SEC to explain the discrepancy, an SEC official said that when they began drafting anti-money laundering exam guidance, SEC representatives were already in contact, and consulting, with Treasury about the new anti-money laundering requirements in the PATRIOT Act. As a result, they were aware that the CIP requirement would be applied to funds. As a result, SEC decided to include guidance, in general terms, for the need for mutual funds to have in place, or start developing, programs to verify the identity of customers.

²²FinCEN said it has limited the scope of financial institutions subject to 314(a) requests primarily to securities broker-dealers, commodity futures commission merchants, and depository institutions primarily to ensure the effective and orderly implementation of the system. Unlike mutual funds, these types of institutions have an existing federal financial regulator that maintains point of contact information. FinCEN has stated that it will consider expanding the universe of financial institutions that receive 314(a) requests in the future if it is feasible and appropriate.

because mutual fund shares are typically purchased through a principal underwriter, which is a registered broker-dealer, most mutual fund accounts would likely be covered by broker-dealers who receive 314(a) information requests.

Development of examination guidance for all of the federal financial regulators and the SROs continues to evolve as events change the requirements financial institutions must adhere to in order to maintain sound anti-money laundering programs. FinCEN is working to provide support to regulators that have been delegated compliance examination responsibilities for financial institutions and has become more involved in helping regulators develop examination guidance and best practices. For example, federal banking regulators, working on an interagency basis through the Federal Financial Institutions Examination Council (FFIEC) and with FinCEN, have drafted joint examination guidance that was being field tested as of March 2005. The targeted issue date for this guidance is June 30, 2005.²³ Banking agency officials told us that this is the first time they have developed joint anti-money laundering guidance and procedures and that they are more comprehensive than any they have issued in the past. As part of this effort, the banking regulators plan to distribute the new examination manual to examiners on a CD that will also include the most current anti-money laundering examination guidance and procedures. SEC officials told us that they also plan to revise the examination guidance and procedures for broker-dealers and mutual funds based on lessons learned from examinations conducted last year. FinCEN officials told us they intend to also work jointly with SEC and CFTC to coordinate efforts among securities and futures regulators and work together on new or revised guidance and procedures. However, FinCEN officials told us that they have not been involved with SEC and CFTC in developing examination guidance to date and they are still in the process of establishing MOUs with the two regulators.²⁴

²³The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. FFIEC was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIR), PL 95-630. OCC, OTS, the Federal Reserve, FDIC, and NCUA constitute the FFIEC.

²⁴According to a recent Department of the Treasury Office of the Inspector General report that reviewed FinCEN's Office of Compliance, the MOU with SEC has been delayed because of fundamental differences.

All of the SROs in our review issued final examination guidance and procedures for the CIP rule and section 314 of the PATRIOT Act. The securities SROs issued final examination guidance for both provisions by October 2003. However, NASD and NYSE began examining firms for compliance with section 314 as early as October 2002 and January 2003, respectively. The futures exchanges jointly issued final guidance for both provisions in February 2004 through a consortium of futures exchanges called the Joint Audit Committee.²⁵ The CFTC, which performs regulatory oversight of the Joint Audit Committee, conducts an annual review of all Joint Audit Committee programs. The anti-money laundering program used by the Joint Audit Committee is among the programs reviewed annually by the CFTC. CME and CBOT had begun assessing firms for account verification, which closely resembles the CIP requirement, by May 2002. NFA updated its guidance to reflect the CIP requirement in October 2003 and April 2003 for section 314 and immediately began assessing firms for compliance with both provisions. NFA officials said they expect to issue revised examination guidance in 2005 for section 326 to address whether, and under what circumstances, an executing broker in a give-up transaction is required to apply its CIP to the give-up customer.²⁶

The federal financial regulators and the SROs included in our review told us they have updated staff about changes to examination guidance and procedures using a variety of techniques including teleconferences, monthly or biannual staff meetings, interagency bulletins, email notifications, and training sessions. For example, banking and securities regulators including the Federal Reserve, OCC, FDIC, SEC, and NASD use teleconferences that are broadcast to headquarters and district offices to update staff on changes to examination guidance, post updates on the organization's Intranet, or use biannual and monthly staff meetings. CFTC and the futures SROs including, CBOT, CME, and NFA update staff through monthly staff meetings and email. NCUA and NYSE send emails to staff that outline or highlight major changes to examination guidance. The

²⁵The Joint Audit Committee is a representative committee of U.S. futures exchanges and regulatory organizations. The committee issues guidance used for futures commission merchants' compliance audits, provides industry updates, and serves as a forum for futures regulators and exchanges to address issues in the commodity and futures industry.

²⁶As noted earlier in this report, give-up relationships occur between carrying brokers and executing brokers when the customer of a carrying broker elects to use an executing broker to place a given trade.

banking regulators also issue agencywide regulatory bulletins and letters to update examiners.

Financial Regulators and SROs Updated Their Training Program and Have Begun to Train Examiners to Evaluate Financial Institutions for Compliance with the CIP Requirement and Section 314

All federal financial regulators and SROs in our review updated their anti-money laundering training to include CIP and section 314. The federal financial regulators and SROs began including CIP and section 314 in training for anti-money laundering examination staff between January 2002 and June 2003. Banking and securities regulators use formal training courses that are both instructor-led and computer-based and industry experts to train staff administering anti-money laundering examinations. Banking regulators also send examiners to training offered by FFIEC. Training at most futures SROs we interviewed is more informal and occurs mostly on the job due to the relatively small examination staffs at these organizations. However, NFA and CFTC offer instructor-led training.

Banking Regulators Use Formal Training Courses and FFIEC to Provide Staff Training

All of the federal banking regulators provide instructor-led courses in anti-money laundering and Web-based training. This training introduces BSA and PATRIOT Act requirements and includes standard presentations and theoretical as well as hands-on training. Their anti-money laundering training curriculum includes instruction in various examination techniques designed to help examiners recognize potential money laundering risks confronting financial institutions and to learn procedures for assessing the soundness of an institution's anti-money laundering program. The federal banking regulators also send staff to conferences sponsored by trade associations that offer multiday focused courses and provide informal resources for self-training such as subscriptions to online newsletters.

However, each banking regulator approaches training differently. For example, OTS and NCUA require all new staff to attend a basic training course in anti-money laundering. According to OTS officials, regional conference training, which is attended primarily by examiners, is an important part of bringing examiners up to speed on anti-money laundering examination procedures. NCUA also uses regional conferences to train large numbers of its examination staff. For example, in 2002, NCUA used regional conferences to provide training on sections 314 and 326 of the PATRIOT Act to all examination staff.

FDIC and the Federal Reserve both have examiners that are anti-money laundering specialists who serve as a training resource to other examiners. Both agencies train examiners who are primarily responsible for conducting anti-money laundering examinations. At the Federal Reserve,

anti-money laundering examination specialists interact on a daily basis with examination staff engaged in anti-money laundering examinations to offer case-specific guidance regarding the requirements. The Federal Reserve also provides on-site examiner training at the individual Reserve Banks, which emphasizes requirements under section 314 and 326 of the PATRIOT Act as warranted. Similar to the Federal Reserve, FDIC uses staff experienced in conducting anti-money laundering examinations as a resource for examiners. Currently, FDIC has 321 anti-money laundering specialists who serve as a resource and as trainers for other examiners. However, FDIC recently trained every examiner on staff, approximately 1,721 as of 2004, in anti-money laundering requirements. In addition, many of its supervisory and legal professionals are pursuing anti-money laundering specialist certifications. OCC has four different training schools, which all provide live, instructor-led training in anti-money laundering requirements. Finally, in an effort to build up staff with anti-money laundering expertise, OCC has a formal on-the-job training program for anti-money laundering and finances certifications in anti-money laundering examination for some of its examiners.

Banking regulators also send examiners to FFIEC's interagency anti-money laundering training workshops. We were able to attend one of these workshops and observed that the course covered the CIP requirement and section 314, in addition to other anti-money laundering requirements. The course included lectures by experienced examiners, presentations by FBI and Internal Revenue Service officials, reading materials, and case study exercises. Many of the case study exercises demonstrated how to identify suspicious transactions and how transaction testing could reveal weaknesses in a financial institution's anti-money laundering program.²⁷ Table 1 provides additional information about training at each of the banking regulators.

²⁷Transaction testing is used to validate examiners' judgment on the reliability of an institution's procedures and internal controls. One form of transaction testing is the comparison of day-to-day practices to the requirements of policies and procedures (to assess compliance with internal systems). This form of testing can reveal whether an institution with sound written procedures has actually incorporated those procedures into its operations.

Table 1: Banking Regulators Anti-Money Laundering Training—2004

Regulator	Training description
OCC	<p>OCC offers instructor-led classroom anti-money laundering training for its examiners at its Consumer Compliance: Basic, Anti-Money Laundering and Terrorist Financing, FinCEN Database Training, and Bank Supervision Schools. As part of OCC's entry-level training, examiners complete 1 week of classroom training and one week of course preparation in the Consumer Compliance: Basic School that includes BSA modules.</p> <p>In 2004, 49 examiners attended the Consumer Compliance: Basic School, 114 attended the Anti-Money Laundering and Terrorist Financing School, 45 attended the FinCEN Database Training School, and 62 attended the Bank Supervision School.</p> <p>In addition to formal course offerings, OCC periodically provides training in the form of agencywide teleconferences and it finances the industry Certified Anti-Money Laundering Specialist certification for some of its examiners.</p>
OTS	<p>OTS requires all examiners administering anti-money laundering examinations to complete 3 weeks of classroom training courses called "Compliance I" and "Compliance II" that includes modules on BSA and the PATRIOT Act.</p> <p>In addition to formal course offerings, OTS provides Web-based anti-money laundering training. In 2004, 463 examiners were trained in anti-money laundering requirements.</p>
NCUA	<p>All new examination staff are required to complete a year-long training curriculum that includes instructor-led training classes and on-the-job training in anti-money laundering.</p> <p>Seasoned examiners are trained on an on-going basis using a combination of instructor-led training sessions and regional conferences. In 2004, NCUA recorded 957 participants in training sessions in anti-money laundering requirements and had 551 examiners on staff. This means that each examiner at NCUA participated in approximately two training sessions in anti-money laundering requirements in 2004.</p>
FDIC	<p>FDIC examiners receive anti-money laundering training in their formal assistant examiner school and formal commissioned examiner school. In 2004, 71 examiners received anti-money laundering training in assistant examiner school and 40 examiners received training in the commissioned examiner school.</p> <p>As of 2004, FDIC trained every examiner on staff (1,721) in anti-money laundering requirements. To meet this requirement, FDIC established a curriculum comprised of several Web-based components. The components are a combination of externally provided courseware, internally developed presentations, and exercises designed to strengthen examiners' knowledge of topics covered.</p> <p>Specialized anti-money laundering training has included outside seminars and conferences, such as industry-sponsored events and regulatory conferences. FDIC also conducts training during examinations. This training is targeted to the individual examiner and addresses the unique business lines and practices at the bank being examined.</p>
Federal Reserve	<p>The Anti-Money Laundering Compliance Section interacts on a daily basis with the examination staff engaged in anti-money laundering examinations at the 12 reserve banks to offer case-specific guidance regarding anti-money laundering requirements.</p> <p>In 2004, the Federal Reserve trained 192 anti-money laundering examination specialists.</p> <p>As part of the Federal Reserve's entry-level training, examiners are required to complete an anti-money laundering online training course.</p>

Source: OCC, OTS, NCUA, FDIC, and Federal Reserve.

Securities Regulators Provide Training to Staff via Formal Instructor-Led Classes and Also Use Industry Experts

Similar to the banking regulators, the securities regulators and SROs also provide formal classroom instruction in anti-money laundering review and some Web-based training, but their approaches differ. SEC provides training to more seasoned staff in anti-money laundering while anti-money laundering training is available to all staff at the securities SROs. However, SEC and NASD are beginning to tailor training in anti-money laundering review for newer staff. For example, beginning in 2005, SEC's training for new examiners will include an anti-money laundering workshop. According to SEC, this effort responds to the increasing importance of anti-money laundering issues and serves to alert less experienced examiners to SEC's new coordination efforts with FinCEN. Similarly, NASD has recently enhanced its new examiner training program through the implementation of a formal classroom training program. As part of this 6-week course, participants will go through 2 full days of training devoted to anti-money laundering requirements, including the CIP requirement and section 314 of the PATRIOT Act. NYSE provides training using a combination of internal and industry experts. Its training program includes several sessions on anti-money laundering and is administered by both internal employees who have an extensive knowledge of the area and outside experts from law and accounting firms.

Securities regulators also coordinate with each other to provide joint training for their examiners. In February 2005, SEC, NASD, and NYSE prepared a 2-day training session devoted to anti-money laundering requirements. This training included presentations from FBI, FinCEN, industry experts, and officials from each of the three securities regulators. The SROs also work together to provide training about timely and relevant examination and compliance topics. According to NASD and NYSE officials we interviewed, the SROs periodically prepare joint training sessions, which cover topics such as anti-money laundering requirements. Table 2 provides additional information about training at SEC and the securities SROs.

Table 2: Securities Regulators Anti-Money Laundering Training–2004

Regulator/ SRO	Training description
SEC	<p>Formal instructor-led training is provided in two different curriculums called “Phase II” and “Phase III.” Training is geared toward more seasoned and mid-level staff. In 2004, SEC trained 237 of these staff in anti-money laundering requirements.</p> <p>SEC’s Joint Regulatory Training Program, which is coordinated with NYSE and NASD, brings exam staff from all three regulators together to discuss and learn about regulatory issues in the securities industry including anti-money laundering requirements.</p>
NASD	<p>Most training is available online and there is also significant formal classroom training. NASD also sponsors symposiums and seminars on anti-money laundering requirements for broker-dealer examinations.</p> <p>As of October 25, 2004, new or inexperienced examination staffs can participate in a 6-week course through NASD’s Examiner University, which devotes 2 days to anti-money laundering requirements.</p>
NYSE	<p>Formal instructor-led training on anti-money laundering is part of the exchange’s ongoing “Regulatory Training Program,” which uses internal and external speakers such as industry experts to present information to staff on important anti-money laundering issues as they relate to examination and enforcement.</p>

Source: SEC, NASD and NYSE.

Futures SROs Provide Instructor-Led and On-the-Job Training

Futures SRO officials at CBOT and CME told us that anti-money laundering training was conducted primarily on the job because these organizations have relatively small examination staffs. According to officials at these organizations, more seasoned, senior staff is responsible for training new staff on how to conduct anti-money laundering reviews. NFA also provides on-the-job training; however, all examiners are required to attend formal training in anti-money laundering such as instructor-led training sessions and technical roundtables on various anti-money laundering issues. In June and July 2004, the NFA’s compliance department conducted two technical roundtables, which focused primarily on CIP requirements. In addition to in-house training, NFA also hosts outside agencies, such as FinCEN, to make presentations on relevant and timely issued related to anti-money laundering requirements. NFA invites other futures SROs including CME and CBOT to most of their training sessions. According to officials at all of the futures SROs, on-the-job and formal, classroom training for examination staff on the CIP requirement and section 314 started as early as May 2002. The CFTC also provides in-house training opportunities for its entire staff, which includes examiners who conduct oversight

examinations of SROs. The training covers all aspects of the anti-money laundering regulatory requirements applicable to futures firms.

Examinations and Enforcement Actions Highlight Progress and Difficulties in Overseeing Compliance with the CIP Requirement and Section 314

The federal financial regulators and SROs responsible for examining financial institutions' compliance with anti-money laundering laws and regulations have conducted examinations that cover compliance with, and have taken enforcement actions concerning, violations of both the CIP requirement and section 314 and its corresponding regulations, but coverage of these requirements varied in the examinations we reviewed. Most of the examinations in our sample assessed whether financial institutions had developed CIPs and procedures for complying with the regulations implementing section 314(a), but specific aspects of the procedures reviewed were not always documented. Some examinations highlighted the difficulties examiners and financial institutions have encountered in understanding CIP requirements. Compliance with section 314(b) and the implementing regulations was not routinely assessed in part because information sharing under 314(b) is voluntary. The regulators and SROs used informal actions to address the deficiencies or apparent violations identified in the examinations in our sample. Since the regulations became effective, some of the regulators have also taken formal enforcement actions that include violations of the CIP requirement and the regulations adopted under section 314(a). Finally, in conducting our work for this objective, we encountered difficulties in obtaining the information on examinations and violations from two of the regulators that revealed weaknesses in their processes for tracking anti-money laundering compliance.

Most Examinations in Our Sample Reviewed CIP, but Coverage of Certain Aspects Varied

As shown in table 3, about 95 percent of the examinations in our sample (168 of 176) documented some type of review of financial institutions' CIP procedures. However, coverage varied when we looked for (1) evidence that the examiner reviewed CIP and (2) documentation of specific aspects of the examiners' reviews, such as reviewing the financial institution's methods of verifying customers' identities or testing the CIP procedures. When we reviewed the examinations for coverage of the CIP requirement, we specifically looked for documentation that the examiner assessed whether (1) the financial institution had developed a CIP and written procedures for CIP; (2) the CIP procedures included collecting appropriate customer information including the minimum requirements, such as date of birth for individuals; (3) the CIP procedures included verifying customer

information using documentary or nondocumentary methods; (4) the financial institution was using risk-based procedures for verification, such as determining how much information to verify depending on its assessment of the risk of the customer or type of account or collecting additional information; and (5) the CIP had been adequately implemented by testing a sample of accounts.

Generally, we saw documentation showing that examiners reviewed the financial institution's written CIP procedures. Most examinations in our sample had evidence that the review included assessing written procedures for CIP (157 of 176 or 89 percent), and the procedures included appropriate customer identification information (144 of 176 or 82 percent) and methods of verification (143 of 176 or 81 percent). Fewer examinations—approximately 56 percent (99 of 176)—assessed whether the financial institution was using a risk-based approach. Our review leads us to believe that the risk-based aspect of CIP is an area that could be difficult for both financial institutions and examiners to interpret consistently, because determining the level of risk of a customer or account can be difficult and depends on several factors, such as the customer's line of business, the process used to open the account, and whether the customer is in the United States or overseas.

Because it can be difficult to determine the customer's risk level, it is not surprising that some examiners would focus on reviewing the minimum requirements, such as the requirements to collect minimum information on customers. OCC officials told us that they developed some internal guidance to assist OCC examiners in understanding the risk-based aspect of CIP early in 2004 because some examiners were confused about it. This guidance explained that limited identification and verification procedures may be appropriate for local residents and businesses, but enhanced procedures may be needed for nonlocal customers, non face-to-face customers (such as customers who conduct transactions by mail, telephone, and Internet), and high-risk accounts (such as private investment corporations, offshore trusts, and foreign customers). The guidance also provided examples of types of enhanced verification procedures, such as customer callbacks, credit verification, and on-site visits that could be used to verify the identity of higher-risk customers. Finally, the guidance stated that for most banks a single set of procedures for verifying the identity of customers would not be adequate. FDIC had also incorporated some examples in examination guidance updated in December 2004 that included examples of how CIP procedures may differ depending on the risk of the customer or type of account. One example in

FDIC's guidance explained when a bank may want to obtain more information on a business or company. The guidance said that although obtaining information on signatories, beneficiaries, principals, and guarantors is not a minimum requirement for CIPs, in the case of opening an account for a relatively new or unknown firm, it would be in the bank's interest to obtain and verify a greater volume of information on signatories and other individuals with control or authority over the firm's account. It is important that examiners determine whether financial institutions have developed risk-based procedures in addition to developing procedures that meet the minimum requirements, because (1) the regulations require that financial institutions develop risk-based procedures and (2) the risk-based procedures allow for more rigorous verification procedures on those types of customers thought to be more at risk of engaging in money laundering or terrorist activities.

Table 3: Coverage of CIP in Our Sample of Examinations Conducted between October 1, 2003, and May 31, 2004

Regulator or SRO	Number of examinations in sample	Evidence that CIP was generally reviewed
Banking		
FDIC	20	20
Federal Reserve	20	20
NCUA	20	20
OCC	20	17
OTS	16	14
Securities		
SEC—Broker-Dealers	11	11
SEC—Mutual Funds	6	5
NASD	20	20
NYSE	21	19
Futures		
NFA	18	18
CBOT	2	2
CME	2	2
Total	176	168 (95%)

Source: GAO analysis of examination sample.

The results of our review of examinations showed considerable variation when we looked for documentation showing whether the examiner tested CIP procedures. We found that only about 43 percent (75 out of 176) examinations tested procedures, in part because our review looked at examinations during the early implementation phase and the examination guidance issued by some regulators does not require that they test procedures. Federal Reserve and FDIC officials said that during the early phase of implementation examiners may have focused on reviewing the procedures with the intent of testing procedures in the next examination cycle. SEC officials said that since many of their broker-dealer examinations that we reviewed were oversight examinations of examinations conducted by NASD or NYSE, SEC examiners would not always conduct testing. Officials from NASD and NYSE told us that some of the smaller broker-dealers may not have opened any new accounts between October 1, 2003, and the time of the examination and, therefore, the examiner would not have tested accounts. NYSE officials also said that CIP was not reviewed in one examination in our sample because the examiner determined that the firm did not have any customers and did not interact with the public.

The regulators and SROs varied in their examiner guidance for testing procedures. The banking regulators use a risk-based approach to their examinations that determines what procedures are performed. Under this risk-based approach to examinations, the examiners first determine whether the financial institution has a strong compliance program and a history of compliance and then tailors the examination procedures based on this risk assessment and review of past examinations. For example, Federal Reserve officials explained that an examiner's review of the independent testing of an institution's anti-money laundering procedures may reduce the need for the examiner to also test certain procedures.²⁸ When the banking regulators issued their joint examination guidance and procedures for CIP in July 2004, the guidance directed examiners to determine whether and to what extent to test CIP procedures based on a risk assessment, prior examination reports, and a review of the bank's audit findings. Although the SEC examination procedures for broker-dealers that

²⁸Section 352 of the USA PATRIOT Act requires that financial institutions have an independent audit function to test its anti-money laundering program. Therefore, examiners would typically review this independent testing and such testing could cover CIP since financial institutions that are subject to both the anti-money laundering program requirement and the CIP requirement must include their CIP as part of their anti-money laundering program.

we reviewed did not include procedures for testing, an SEC official told us that the initial request letters sent to institutions include a request for customer account information so that examiners can test those accounts for CIP compliance. SEC's procedures that we reviewed for mutual funds included procedures for sampling accounts and testing CIP procedures for examinations of funds' transfer agents that maintain customer account information.²⁹ NASD and NYSE have instructions that include sampling accounts to determine whether the financial institution's CIP procedures are being implemented properly. The examination procedures used by NFA and the futures exchanges also include procedures to test the CIP procedures against a sample of high-risk accounts.

We also looked to see if examiners conducted any testing of high-risk accounts because the results of such testing would provide a clearer indicator of whether the financial institution was exercising more due diligence on riskier accounts.³⁰ We saw evidence that examiners tested a sample of high-risk accounts for CIP compliance in 8 of 176 of the examinations. Several regulatory officials told us that the institutions in our sample may not have had high-risk accounts. For example, many of the NFA examinations included documentation saying that the institution did not have any high-risk accounts and therefore a sample of such accounts were not tested. Also, NCUA and OTS officials said that the probability that the institutions they regulate would have high-risk accounts was small.

Although most of the examinations had documentation that the examiner had reviewed CIP, the documentation, such as the examination report or a summary written by an examiner, did not always specify how the review was conducted.³¹ Therefore, some of the variation in the results from our examination review may also be due to differences in the way examiners document their work. We observed a variety of methods for documenting

²⁹Transfer agents are not subject to a CIP requirement unless they are a bank or a broker-dealer, although many of them perform CIP requirements as a service to their affiliated mutual funds and broker-dealers.

³⁰According to the CIP examination procedures issued by the banking regulators, high-risk accounts may include, but are not limited to, foreign private banking and trust accounts, offshore accounts, and out-of-area and non face-to-face accounts.

³¹In determining whether the examination documented a review of CIP and section 314, we reviewed examination reports, written summaries of examination findings, questionnaires or worksheets used by examiners to record their work, and workpapers that may include copies of the financial institution's procedures, internal audits, records of transaction testing, and memorandums.

examination procedures that were conducted and examination results. Some of the federal financial regulators and SROs used a system of recording the completion of examination procedures, such as a questionnaire or worksheet, which generally made it easy to follow what the examiner had done but did not always include the same aspects that we were reviewing. For example, NCUA examiners document their examinations using a questionnaire. However, this questionnaire does not ask the examiner to document whether he or she tested CIP procedures. In the one instance in which we saw documentation of testing by NCUA, the NCUA examiner had documented a deficiency in the credit union's CIP procedures based on looking at a sample of accounts. An FDIC official told us that examiners may not document that they tested procedures unless it showed a deficiency. Some examiners documented their review by making notes on copies of the financial institution's procedures. Finally, some examinations, such as a few of the examinations conducted by the Federal Reserve and OCC, used memorandums that discussed the findings of the examination. However, the memorandums may not have specified all of the aspects of CIP that were reviewed. In addition, OCC officials told us that OCC does not require examiners to document every procedure that they complete or what they do not do in an examination.

The Results of Our Examination Review Highlighted Some Difficulties in Understanding CIP Requirements

Our review of some of the examinations in the sample revealed that examiners and financial institutions may not always understand the requirements for CIP or interpret them in the same way. The aspects of CIP that raised questions about whether examiners or financial institutions understand them are (1) the differences between CIP and know-your-customer procedures; (2) the differences between the requirements to check government lists for CIP versus other government lists such as OFAC; and (3) the extent to which a financial institution performs CIP procedures for existing customers. Some confusion or lack of understanding is to be expected during the early phases of implementing new requirements. However, these differences in understanding have resulted in inconsistencies in the examination process and may have created further confusion and misunderstandings.

CIP and Other Procedures That Require Customer Identification

A potential challenge to assessing compliance with CIP are the similarities among CIP requirements and other procedures that require customer identification for anti-money laundering purposes, including what has been called "know-your-customer" or "customer due diligence" (CDD) procedures. Also, although not an issue in the examinations we reviewed, section 312 of the PATRIOT Act adds another customer due diligence

requirement and could lead to misunderstandings about appropriate due diligence. Section 312 requires appropriate, specific and, where necessary, enhanced, due diligence for correspondent accounts and private banking accounts established in the United States for non-U.S. persons.³² FinCEN adopted an interim final rule for section 312 on July 23, 2002. In the interim rule, FinCEN noted that the requirements of this provision placed on financial institutions are significant and therefore, additional time was necessary to consider what is appropriate for the final rule.

As shown in table 4, CIP, know-your-customer procedures, and section 312 have some similarities. All three require some level of collecting customer identification information and taking steps to verify that information and the risk-based aspect of CIP could overlap or duplicate know-your-customer procedures and section 312 requirements. However, know-your-customer procedures typically require more information than CIP. According to the 1997 BSA examination manual issued by the Federal Reserve, a know-your-customer policy begins with obtaining identification information and taking steps to verify information—similar procedures to CIP. However, know-your-customer procedures also include obtaining information on the source of funds used to open an account and determining whether to obtain information on beneficial owners of certain types of accounts such as trusts. One goal of know-your-customer procedures is to collect sufficient information so that the financial institution knows what to expect in terms of customer account activity so that it can adequately monitor for unusual or suspicious activities.

³²U.S.C. § 5318(i).

Table 4: Anti-Money Laundering Policies That Depend on Procedures to Verify Customer Identities

Anti-Money laundering policy	Description of the procedures	Rationale for procedures
Customer Identification Program (CIP)	<ul style="list-style-type: none"> • Minimum requirements include customer name, date of birth, physical address, and government-issued ID number. • Identification verification procedures are risk-based. 	Collecting identification information and verifying customers' identities make it more difficult for money launderers and other criminals to use the U.S. financial system and should provide useful information to law enforcement if the customer becomes a suspect in an investigation.
Know-Your-Customer	<ul style="list-style-type: none"> • Identification information is collected, but there are no minimum requirements. • Customer information usually includes source of funds and information on beneficial owners of certain accounts. • Procedures include taking steps to verify the identity of the customer. 	Information on a customer's identity and expected transactions enables the institution to effectively monitor for suspicious transactions and comply with requirements to report suspicious activity reports.
Due Diligence for Private Banking Accounts of Non-U.S. Persons ^a	<ul style="list-style-type: none"> • Minimum requirements include identifying the nominal and beneficial owners of, and the source of funds deposited into such an account. • Enhanced scrutiny of accounts held by or on behalf of a senior foreign political figure or any immediate family member or close associate. • Procedures are risk-based. 	Due diligence procedures are intended to guard against money laundering and enable the financial institution to report any suspicious transactions related to types of accounts that have been known to be used for money laundering.

Source: GAO analysis.

^aSection 312 requires that banks also conduct due diligence for foreign correspondent accounts whereas the private banking requirement applies to banks and broker-dealers. For the purpose of illustrating how the different rules' requirements are similar without becoming too complicated, we are only showing the requirement for private banking accounts of non-U.S. persons.

In 6 examinations in our sample of 176, we found evidence that examiners were confusing know-your-customer procedures with CIP. For example, in 1 examination, the examiner documented a review of CIP but the documentation included a copy of the financial institution's know-your-customer procedures that had been in place since 1997 and had not been updated to include the minimum identification standards and other CIP requirements, such as recordkeeping procedures. As a consequence, this institution may be doing less than what CIP requires. In another examination, the examiner reviewed the institution's know-your-customer procedures, which included the minimum CIP requirements but also directed employees to do more due diligence than CIP may require depending on a risk assessment of the account and customer. As a consequence the examiner and institution may believe that compliance with CIP requires more procedures than necessary. Draft examination guidance that the banking regulators intend to issue in June 2005 may improve understanding of the difference. The draft guidance explains that

customer due diligence begins with customer identification and verification but also involves collecting information in order to evaluate the purpose of the account to be able to detect, monitor, and report suspicious activity. One regulatory official told us that the banking regulators now refer to know-your-customer procedures as “customer due diligence.”

CIP Requirements for Checking Government Lists

In 7 examinations, we found that the examiner confused the CIP requirement to check government lists of suspected terrorists with another government requirement to freeze assets and block transactions of designated persons and entities. Treasury’s Office of Foreign Assets Control (OFAC) requires financial institutions to freeze assets or block transactions of people and entities on the List of Specially Designated and Blocked Persons.³³ Therefore, financial institutions check customers against this list to ensure that they are in compliance. In these 7 examinations, the examiners noted that the financial institution was not compliant with the CIP requirement to check government lists because the institution was not checking customers against the OFAC list. However, as FinCEN and the banking regulators noted in the first set of CIP FAQs, lists published by OFAC whose independent requirements stem from statutes other than the PATRIOT Act and are not limited to terrorism, have not been designated for purposes of the CIP rule.

Applying CIP to Existing Customers

Two examinations documented disputes or confusion about the extent to which financial institutions should apply the CIP requirement to existing customers who open new accounts. In one examination, the examiner cited a CIP deficiency because the institution had not updated the address information for all of its existing customers. However, the CIP rule only applies when an existing customer is opening a new account and the CIP rule does not expect institutions to update records on existing customers if it has a reasonable belief that it knows the true identity of its customers. As stated in FAQs for the CIP rule issued by FinCEN and the banking regulators, a bank can demonstrate it has a reasonable belief that it knows its customers’ true identities if it had comparable procedures in place prior to October 1, 2003, or provide documentation showing that it has had a

³³OFAC administers and enforces economic and trade sanctions against countries and groups of individuals, such as terrorists and narcotics traffickers. OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are to be blocked and U.S. persons are generally prohibited from dealing with them.

long-standing relationship with a particular customer. In the other examination, the institution and the examiners were familiar with the CIP requirements but differed in interpreting the extent to which an institution can develop a policy that exempts existing customers who open new accounts. The institution disputed the examiners' finding that it was not in compliance with CIP because it had assumed it knew the identity of all of its customers who had opened accounts prior to January 2000. The institution argued that it had procedures in place prior to 2000 that were similar to CIP procedures and therefore did not have to apply the CIP requirement to existing customers who open new accounts.

Most Examinations in Our Sample Covered Section 314(a), While about Half Covered Section 314(b) in Part Because It Is Voluntary

As shown in table 5, most of the examinations in our sample—about 76 percent—included a review of compliance with section 314(a), but documentation of specific aspects of section 314(a) were somewhat less. We found documentation in 58 percent (91 of 157) of the examinations in which the examiner determined that the financial institution was receiving 314(a) information requests from FinCEN. We also looked for evidence of whether the examiner tested the 314(a) procedures and found documentation of testing for about 16 percent (25 of 157) of the examinations.

Although many of the examinations had documentation that the examiner had reviewed section 314(a), the documentation, such as the examination report or a summary written by an examiner, did not always provide enough specificity for us to determine if the examiner had verified that the financial institution was receiving the requests or tested the procedures. Also, in some cases, the examination procedures did not require that examiners test 314(a) procedures. Neither NFA nor the exchanges require in their examination guidance that examiners test the 314(a) procedures to check if all of the required types of records are searched, but they do require that the examiner determine if the financial institution responded within 2 weeks if it had a customer account that matched a subject on the 314(a) request. An SEC official told us that it would be difficult to test the 314(a) procedures in many cases because many financial institutions destroy the 314(a) information requests after they have searched their accounts. The examination procedures for section 314(a) issued by the banking regulators are also conducted under a risk-based approach. Under the risk-based approach, examiners may determine the need to select a sample of positive matches or recent 314(a) requests to test the procedures.

Table 5: Coverage of Section 314(a) in Our Sample of Examinations Conducted between October 1, 2003, and May 31, 2004

Regulator or SRO	Number of examinations in sample	Evidence that section 314(a) was generally reviewed
Banking		
FDIC	20	19
Federal Reserve	20	18
NCUA	20	20
OCC	20	7
OTS	16	14
Securities		
SEC—Broker-Dealers ^a	11	8
NASD	20	18
NYSE	21	12
Futures		
NFA ^b	5	2
CBOT	2	0
CME	2	2
Total	157	120 (76%)

Source: GAO analysis of examination sample.

^aThe SEC sample for section 314(a) excludes examinations of 6 mutual fund entities.

^bThe NFA sample for section 314(a) excludes examinations of 15 introducing brokers.

The samples for SEC and NFA are smaller in our review of section 314(a) because certain types of financial institutions do not typically receive the 314(a) information requests from FinCEN. According to SEC and FinCEN officials, under the 314(a) process, information requests are generally sent out to banks, credit unions, broker-dealers, and futures commission merchants because these types of financial institutions have an established infrastructure for capturing point of contact information. Also, SEC officials told us that because mutual fund shares are typically purchased through a principal underwriter, which is a registered broker-dealer, most mutual fund accounts would likely be covered by broker-dealers who receive 314(a) information requests. Therefore, SEC does not examine mutual funds for compliance with section 314(a) at this time. SEC officials said that because many of the examinations of broker-dealers in our sample were oversight examinations of NASD and NYSE, some examinations

would not necessarily review all aspects of a financial institution's anti-money laundering program.

The number of examinations in our sample of NFA examinations that covered section 314(a) is fewer than for CIP because most of the examinations included in our NFA sample were examinations of introducing brokers. NFA officials explained that introducing brokers do not typically receive 314(a) requests because under industry regulation every customer of an introducing broker must also be a customer of a futures commission merchant. Therefore, if introducing brokers were required to conduct 314(a) searches, they would be searching the same universe of customers covered by the 314(a) requests sent to futures commission merchants. Also, two of the NFA examinations of futures commission merchants did not cover section 314(a) because (1) NYSE and NASD had recently examined one of the firms and had covered it and (2) NFA limited the scope of the examination of the other firm based on prior NFA examinations that found the procedures were adequate. The two CBOT examinations did not cover section 314(a) because the examinations we reviewed were conducted prior to the issuance of the futures exchanges' revised examination guidance and procedures in February 2004 that were updated to include section 314(a).

Some of the OCC and NYSE examinations also did not cover a review of section 314 procedures because our review occurred during the early implementation phase and their examination approaches were still evolving. According to OCC officials, OCC examinations in our sample did not always cover section 314(a) procedures because during this time period OCC was in the process of implementing its approach to reviewing the PATRIOT Act provisions. In February 2004, OCC issued guidance to its examiners to identify those banks with a high risk money laundering profile with the intent of giving those institutions a higher priority in the examination cycle for covering the PATRIOT Act provisions. Because OCC examiners were just beginning to review the PATRIOT Act provisions during the time of our review, some examinations may have not covered all aspects of the PATRIOT Act. OCC officials also said that some examiners may have focused on CIP because CIP procedures are more complex. OCC officials said that compliance with section 314 and the CIP requirement would be examined in all large banks by March 2005 and in all small and mid-sized banks by end of 2006. NYSE examinations did not always cover section 314(a) procedures, in part, because NYSE examination procedures were not clear about how examiners should review section 314(a) procedures. Initially, NYSE had included an examination procedure

covering section 314(a) within its examination objective covering the firm's anti-money laundering program. NYSE officials created a separate examination objective for section 314(a) while we were conducting our review and told us that the revised questions and procedures were incorporated into the anti-money laundering examination module in December 2004.

As shown in table 6, about 55 percent of the examinations in our sample covered section 314(b). The sharing of information with other financial institutions pursuant to section 314(b) is voluntary. As a consequence, some examiners may have chosen not to examine _ for compliance with section 314(b) regulations and some federal financial regulators and SROs did not develop examination procedures for determining compliance with section 314(b) regulations. SEC did not include section 314(b) in its examination procedures for mutual funds because it is voluntary. The futures SROs—NFA, CME, and CBOT—also did not include procedures for examining compliance with section 314(b) regulations. An NFA official told us that they did not review 314(b) because it is voluntary. Most of the regulators and SROs that examined section 314(b) procedures emphasized in their guidance that the provision is voluntary and financial institutions can choose not to share customer information with other financial institutions or share customer information without the benefit of the safe harbor. However, financial institutions may choose to share information without providing notice to FinCEN and be at risk of violating privacy laws. An NYSE official told us that they assess compliance with section 314(b) regulations to ensure that the financial institution will not violate privacy laws. The procedures issued jointly by the federal banking regulators state that the failure to follow the section 314(b) procedures is not a violation of section 314(b) but could lead to a violation of privacy laws or other laws and regulations.

Table 6: Coverage of Section 314(b) in Our Sample of Examinations Conducted between October 1, 2003, and May 31, 2004

Regulator or SRO	Number of examinations in sample	Covered section 314(b)
Banking		
FDIC	20	11
Federal Reserve	20	8
NCUA	20	20
OCC	20	4
OTS	16	11
Securities		
SEC—Broker-Dealers	11	7
SEC—Mutual Funds	6	0
NASD	20	16
NYSE	21	20
Futures		
NFA	18	0
CBOT	2	0
CME	2	0
Total	176	97 (55%)

Source: GAO analysis of examination sample.

Federal Financial Regulators and SROs Generally Used Informal Actions to Address CIP and Section 314(a) Deficiencies and Violations

Because the regulations were new and many deficiencies and violations were technical mistakes, the federal financial regulators and SROs mostly took informal actions³⁴ to address deficiencies and apparent violations associated with section 314 and CIP. In our sample of 176 examinations, 32 examinations reported deficiencies or apparent violations related to section 314(a) and 79 examinations reported deficiencies or apparent violations relating to CIP requirements.

The federal financial regulators and SROs used different terms to classify problems associated with section 314 and CIP and other elements of institutions' anti-money laundering programs. For example, some regulators would generally identify section 314 or CIP problems as "violations" or "apparent violations," while some of the banking regulators would use the term "deficiency" in some cases and "violation" in other cases. Officials from one of the banking regulators told us that they are in the process of developing guidance on the matter. To allow for comparison and aggregation across the different regulators and SROs, we examined problems identified as both violations and deficiencies for our analysis. The varying terminology has an impact on the banking regulators' reporting systems, since some regulators track apparent violations but do not track deficiencies. This issue will be examined in more depth in other work we are conducting on the banking regulators and BSA examinations and enforcement.

The types of section 314(a) deficiencies and violations in our sample varied. Table 7 lists examples of the types of deficiencies and violations in the examinations we identified as being minor or significant. We defined those deficiencies and violations as minor when the financial institution was generally receiving 314(a) requests and searching its accounts, but its procedures needed enhancements. Those deficiencies and violations that we defined as significant were situations in which the institution was not receiving 314(a) requests or adequately searching accounts.

³⁴Regulators may use an informal action when a financial institution's overall condition is sound, but it is necessary to obtain written commitments to ensure that identified problems and weaknesses are corrected. Agreement to an informal action can be evidence of a commitment to correct identified problems before they adversely affect an institution's performance or cause further decline in its condition. Informal enforcement actions include commitment letters, deficiency letters, and memorandums of understanding.

Table 7: Examples of Minor and Significant 314(a) Deficiencies and Violations Identified in the Sample

Minor deficiencies and violations	Significant or major deficiencies and violations
<ul style="list-style-type: none"> Point of contact information was incorrect; and Institution had not formalized its 314(a) procedures. 	<ul style="list-style-type: none"> Institution's point of contact was not receiving 314(a) requests; and Institution did not have internal procedures in place to respond to 314(a) requests.

Source: GAO analysis of examination sample.

The severity of CIP deficiencies and violations also varied. We defined CIP deficiencies and violations as being minor when the financial institution generally had CIP procedures, but some aspects needed enhancements or were incomplete according to the regulatory requirements. Situations in which the institution did not have any CIP procedures or the examiner found that the institution was generally not following its CIP procedures we defined as significant. Table 8 lists some examples of minor and significant CIP deficiencies and violations in our sample of examinations.

Table 8: Examples of Minor and Significant CIP Deficiencies and Violations Identified in the Sample

Minor deficiencies and violations	Significant or major deficiencies and violations
<ul style="list-style-type: none"> CIP testing is not included in the institution's BSA/AML audit plan; CIP policy did not adequately address when it will rely on another firm to perform customer identification procedures; Institution did not provide adequate notice to customers that the bank will gather personal information to verify their identities; and Institution failed to develop and adopt a board approved, written CIP; although institution was in compliance with the substance of section 326. 	<ul style="list-style-type: none"> Institution did not follow its identification verification procedures; and Institution did not have a CIP.

Source: GAO analysis of examination sample.

In many cases, the examinations included documentation showing that institution management agreed to correct deficiencies or violations. In several instances, the examination included documentation in which the

board of directors of the institution is directed to address the deficiencies. For example, the Federal Reserve required a board of directors to address a bank's failure to maintain documentation of its 314(a) searches and to address the violation within 30 days of the examination. Similarly, NCUA noted that a credit union lacked CIP policies and procedures and directed its board of directors to address the apparent violation within a specific timeframe. Additionally, in a few cases, examiners documented that deficiencies or violations were corrected during the exam. For example, a financial institution examined by NASD updated its procedures for addressing FinCEN information requests while examiners were on-site.

Recent Formal Enforcement Actions Have Cited Violations of CIP and Section 314(a)

Although none of the examinations in our sample resulted in formal enforcement actions,³⁵ recent formal enforcement actions involved violations of the CIP requirement and the regulations under section 314(a). The federal financial regulators have independent statutory authority to institute formal enforcement actions themselves, and they may also refer BSA violations to FinCEN for formal enforcement action.³⁶ Under delegated authority, FinCEN is the administrator of the BSA and has the authority to enforce BSA regulations.³⁷ FinCEN's Office of Compliance and Regulatory Enforcement evaluates enforcement matters that may result in a variety of remedies, including the assessment of civil money penalties.

The federal banking regulators have the authority to take formal enforcement action if they determine that a financial institution is engaging in unsafe or unsound practices or has violated any applicable law or regulation.³⁸ According to officials from the federal banking regulators,

³⁵Unlike most informal actions, formal enforcement actions are authorized by statute, are generally more severe, and are disclosed to the public. Also, formal actions are enforceable through the assessment of civil money penalties or fines, and, with the exception of formal agreements, through the federal court system. Formal enforcement actions include cease and desist orders and other consent orders and formal written agreements.

³⁶In addition, SRO rules typically provide for institution of enforcement actions against members of the SRO for violation of applicable laws and regulations and for the imposition of sanctions on members for such conduct. SROs can make referrals to the SEC or CFTC for referral to FinCEN.

³⁷See Treasury Department Order No. 108-01, dated September 26, 2002, and 31 C.F.R. 103.56. The Secretary is authorized to delegate such responsibilities to FinCEN pursuant to 31 U.S.C. § 310 (b)(2)(i) and (J).

³⁸12 U.S.C. § 1818(b).

they would take formal action, such as issuing a cease and desist order, if they detected systemic or willful violations of the BSA.³⁹ Violations of formal agreements or orders, such as a cease and desist order, may result in the assessment of civil money penalties. According to a September 2004 MOU among the federal banking regulators and FinCEN, the federal banking regulators have agreed to promptly notify FinCEN of significant BSA violations or deficiencies by financial institutions under their jurisdiction.⁴⁰ SEC officials said that significant and willful BSA violations would be referred to its enforcement division, as well as FinCEN.⁴¹ Similarly, NASD and NYSE have their own rules to enforce anti-money laundering regulations⁴² and officials from NASD and NYSE said that they would take formal actions and may make a formal referral to FinCEN if they encountered certain BSA violations. Officials from CFTC and the three futures SROs in our review also said that they would take formal action for significant BSA violations under their own rules to enforce anti-money laundering regulations as well as refer the violations to FinCEN.⁴³

We identified several formal enforcement actions taken by the federal banking regulators and FinCEN that included violations of CIP that demonstrate how violations of CIP and section 314(a) are enforced (see table 9). Only one enforcement action—AmSouth—included a violation of section 314(a). These enforcement actions generally consisted of civil money penalties, supervisory or written agreements, or cease and desist orders. In each of these actions, the financial institution agreed to comply with the enforcement action.

³⁹A cease and desist order requires an institution to cease and desist from unsafe or unsound practices and may require the institution to take affirmative action to correct the conditions resulting from any such violation or practice.

⁴⁰The MOU specifies that a “significant BSA violation or deficiency” includes systemic or pervasive BSA compliance program deficiencies or reporting or recordkeeping violations, as well as a one-time, nontechnical BSA violation that demonstrates willful or reckless disregard for the BSA requirements or that creates a substantial risk of money laundering or the financing of terrorism within the financial institution.

⁴¹SEC has the authority to take an enforcement action against broker-dealers and mutual funds who violate anti-money laundering regulations set forth in 17 C.F.R. §§ 240.17a-8, and 270.38a-1.

⁴²NASD, Rule 3011(a), (b), (c), (d), and (e); and NYSE, Rule 445.

⁴³CFTC, Rule 42.2; CBOT, Rule 423.05; CME, Rule 981; and NFA, Rule 2-9(c).

Table 9: Recent Enforcement Actions and Civil Money Penalties against Banks That Included CIP and Section 314(a) Violations

Financial institution	Agency	Date	Enforcement action/civil money penalty	CIP or section 314 violation
Abacus Federal Savings Bank	OTS	10/2003	\$175,000 civil money penalty	In the Cease and Desist Order issued on the same day as the civil money penalty, OTS ordered Abacus to implement an adequate AML program that included an adequate CIP.
Fort Lee Federal Savings Bank	OTS	2/2004	Supervisory agreement	As part of the agreement, Fort Lee agreed to update its BSA and OFAC policies and procedures, including its CIP.
BAC Florida Bank	FDIC	4/2004	Cease and desist order	Among other things, FDIC cited the bank for failing to implement an effective customer identification program. The bank was required to develop an effective customer due diligence program and provide for internal controls, independent testing, suitable training, and a BSA officer to ensure compliance.
Hudson United Bank	FDIC	5/2004	Cease and desist order	Among other things, FDIC ordered Hudson to complete a review of its CIP.
Riggs National Bank	OCC and FinCEN	5/2004	\$25 million civil money penalty ^a	In addition to other BSA violations, FinCEN and OCC found that Riggs did not adequately implement enhanced due diligence and CIP programs.
First Midwest Bank	Federal Reserve	7/2004	Written agreement	Bank agreed to submit to the Federal Reserve an acceptable enhanced written customer due diligence program within 60 days of the agreement.
ABN AMRO Bank	Federal Reserve ^b	7/2004	Written agreement	The bank agreed to submit an acceptable written customer due diligence and CIP program within 60 days of the agreement. As part of the program, the bank agreed to determine the appropriate documentation necessary to verify the identity and business activities of its customers.
AmSouth Bank	FinCEN and Federal Reserve	10/2004	\$10 million civil money penalty ^c	AmSouth's AML program lacked adequate internal controls and procedures that were necessary to enable the performance of appropriate customer due diligence, including compliance with section 314(a). AmSouth agreed to submit an acceptable written customer due diligence program within 30 days of the agreement.
First Community Bank	FDIC	10/2004	Cease and desist order	FDIC cited the bank for failing to implement effective customer identification procedures, among other things. Bank required to establish a CIP and 314 information sharing guidelines within 60 days of the order.

(Continued From Previous Page)

Financial institution	Agency	Date	Enforcement action/civil money penalty	CIP or section 314 violation
Beach Bank	FDIC	11/2004	Cease and desist order	Among other things, FDIC cited the bank failing to implement an effective customer identification program. FDIC ordered the bank to develop and implement a written plan for the continued administration of its CIP program and procedures within 60 days of the order.
Liberty Bank of New York	FDIC	11/2004	Cease and desist order	FDIC ordered the bank to revise and enhance its customer identification program and account opening procedures.
Security State Bank	FDIC	12/2004	Cease and desist order	Among other things, FDIC ordered the bank to establish an adequate independent testing program within 60 days of the order. As part of this program, the bank was ordered to test its customer identification program, customer due diligence, and compliance with information sharing requirements.

Source: GAO analysis of regulatory enforcement actions.

^aOCC and FinCEN assessed concurrent \$25 million civil money penalties. The agencies stated that the penalties would be satisfied by one payment of \$25 million to Treasury.

^bThe State of Illinois Department of Financial and Professional Regulation was also part of the written agreement.

^cAmSouth also forfeited \$40 million as part of a deferred prosecution agreement with the Justice Department.

Two of these enforcement actions provide additional examples of how CIP has been confused with know-your-customer policies. In two of the cases above, Beach Bank and BAC Florida Bank, FDIC’s cease and desist orders cited institutions for violations of 31 C.F.R. § 103.121 by “failing to implement an effective customer identification program and/or effective ‘Know Your Customer’ policies and procedures.” While 31 C.F.R. § 103.121 requires banks to implement a CIP appropriate for their size and type of business, it does not require banks to adopt know-your-customer policies and procedures. Know-your-customer procedures generally require more information than CIP.

We also identified five formal enforcement actions brought against broker-dealers for violations of CIP and section 314(a) requirements. According to NASD, the firms that were the subject of the NASD enforcement actions in table 10 were generally firms with limited risk profiles. Most of the firms did not have extensive client bases, a large number of registered representatives, and multiple branch offices. Therefore, the fine amounts reflect both the smaller size and financial resources of the firms and the lower risk of money laundering inherent in their business models.

Table 10: Recent Enforcement Actions against Securities Broker-Dealers That Included CIP and Section 314(a) Violations

Financial institution	Agency	Date	Enforcement action	CIP or section 314(a) violation
Hartsfield Capital Securities Inc.	FinCEN	11/2003	\$10,000 civil money penalty	After identifying violations during an examination, SEC referred this case to FinCEN. FinCEN found that Hartsfield lacked policies, procedures, and internal controls relating to its CIP.
Harrison Securities, Inc.	NASD	12/04	Firm expelled from NASD	Among other things, the firm did not have procedures for responding to 314(a) requests.
Investors Brokerage of Texas, Ltd.	NASD	12/04	\$10,000 fine and censure	Among other things, the firm's AML program did not adequately establish a CIP.
Trident Partners	NASD	2/05	\$17,500 fine and censure	Among other things, the firm failed to receive FinCEN 314(a) notices because it failed to update its AML contact information.
FSC Securities Corp.	NASD	3/05	\$40,000 fine and censure	Among other things, the firm failed to maintain adequate procedures that addressed keeping confidential FinCEN information requests.

Source: GAO analysis of regulatory enforcement actions.

Regulators' Processes for Tracking Examination Information Varied with Some Having Weaknesses That Could Affect Their Ability to Monitor Anti-Money Laundering Compliance

Reviewing examination data and 176 examinations across six regulators and five SROs provided us an opportunity to see a wide range of practices for managing anti-money laundering oversight programs. One of the key practices that varied across programs was the tracking system used to track examination information. The information that was provided to us on the examinations and apparent violations that covered section 314 and CIP raised broader issues about how the regulators and SROs track anti-money laundering compliance information. To select our sample of examinations, we requested information on the examinations and apparent violations that covered section 314 and CIP, but two of the regulators could not easily obtain this information from their tracking systems. Although we assessed the reliability of the data we received, we did not conduct broad assessments of the information systems and processes regulators and SROs use to track examinations in this report, in part, because we have other work reviewing the banking regulators' anti-money laundering examinations and enforcement programs and SEC's examination programs that both include reviewing how they track examinations. However, we highlight the problems we encountered in this review because the problems could affect regulators' ability to monitor compliance with sections 314 and CIP as well as other anti-money laundering requirements.

Generally, OCC, FDIC, OTS, and NCUA were able to respond to our data request using their examination tracking systems and provide information on examinations that would most likely cover section 314 and CIP by identifying examinations that covered anti-money laundering compliance and information on apparent violations. The information varied in determining whether the examinations actually covered CIP and section 314 during the period of time between October 1, 2003, and May 31, 2004, because the regulators began examining for these provisions at different times. For example, OCC's system is designed to capture examination areas but examiners were not provided guidance to begin reviewing PATRIOT Act provisions until late February 2004, and therefore, the system was not always recording that they had performed modules covering the PATRIOT Act sections for the period of our review. Also, NCUA officials told us that we were more likely to be able to review examinations that covered section 314 and CIP in examinations completed on or after February 2004, because those examinations were more likely to have used the revised examination questionnaire for anti-money laundering compliance that had been installed on computers in December 2003.

The Federal Reserve had some difficulty responding to our request because the Federal Reserve's existing automated tracking system for examinations did not capture sufficient detail on whether its examinations cover a review of anti-money laundering compliance. Although full-scope examinations are all supposed to cover anti-money laundering compliance, many of the Federal Reserve's target examinations may also cover anti-money laundering compliance, but their tracking system does not capture this level of detail. Therefore, the Federal Reserve could not readily identify the population of examinations that would most likely cover CIP and section 314. Also, although the Federal Reserve tracks information on apparent violations, its tracking system does not track deficiencies. This distinction was important to our information request because the Federal Reserve had not had any apparent violations related to section 314 or CIP, but its Federal Reserve Banks had reported deficiencies in quarterly reports to the Federal Reserve Board. However, the information in the quarterly reports was not sufficiently detailed enough for identifying specific examinations that had deficiencies related to CIP or section 314. Therefore, the Federal Reserve Board had to request this information from the 12 Federal Reserve Banks who had to manually go through examination files and compile the information. Federal Reserve officials told us that they are making significant enhancements to the tracking system to capture additional information on Bank Secrecy Act and anti-money laundering compliance.

SEC's examination tracking system is supposed to capture information on whether the examination included certain focus areas, such as a review of anti-money laundering compliance. However, when attempting to respond to our information request on broker-dealer examinations, SEC discovered that the information from its tracking system did not appear to be accurate. According to an SEC official, SEC information on anti-money laundering examinations for broker-dealers was not always accurate because examiners were not always inputting all of the focus areas that they covered, including anti-money laundering. Therefore, SEC conducted a word search through its database of examination reports to identify examinations that covered section 314 and CIP and identified about 26 examinations to respond to our information request. After our data request, SEC officials emailed a reminder to examination staff of the importance of accurately filling out all examination information in the tracking system, including identifying when anti-money laundering is a focus area, and asked that they review the accuracy of this information for completed examinations and update it as necessary. For mutual fund examinations, SEC used the same tracking system to identify all routine examinations of mutual funds during our examination review period because anti-money laundering was expected to be a focus area for all routine examinations and did not encounter the same problem. NASD and NYSE were able to identify examinations and apparent violations of section 314 and CIP using their examination tracking systems.

The futures SROs provided us information without any difficulty. According to an NFA official, once NFA had identified through its tracking system the population of examinations that covered anti-money laundering compliance and those examinations that included an apparent violation, the examinations were reviewed to identify whether the apparent violation was related to section 314 or CIP. CME and CBOT each only have approximately 30 to 40 futures commission merchants at any point in time that they track and had only completed a few examinations during the time period for our examination review and therefore did not have difficulty responding to our information request.

Law Enforcement Officials Believe That Section 314(a) and CIP Have Been Valuable Tools in Terrorist and Money Laundering Investigations

Law enforcement officials praised the 314(a) process, stating that it has improved coordination between law enforcement agencies and financial institutions and indicated that CIP has also assisted investigations. The 314(a) process has resulted in discovery of additional accounts held by suspects and issuance of grand jury subpoenas, search warrants, arrests, and indictments. Most law enforcement officials we interviewed also believed that CIP requirements have helped investigators by ensuring that better and more detailed information is collected and maintained at financial institutions. Although CIP and 314(a) processes are useful tools for investigating money laundering and terrorist financing cases, the decision to bring charges in specific cases is always discretionary.

Law Enforcement Officials Believe That the Section 314(a) Process Has Improved Coordination with Financial Institutions and Has Led to More Efficient Investigations

Officials from the Department of Justice and other law enforcement agencies told us that the 314(a) process has improved coordination between law enforcement agencies and financial institutions and has increased the speed and efficiency of investigations. Department of Justice officials, including supervisory prosecutors in two U.S. Attorneys Offices, with whom we spoke, said that the 314(a) process facilitated the flow of information between financial institutions and law enforcement officials by connecting FinCEN to approximately 20,000 financial institutions.

Investigators use the information FinCEN gathers from these financial institutions as evidence in building cases against potential money launderers and terrorist financiers. FinCEN recently reported that the 314(a) system has processed 381 requests since it resumed operation in February 2003. Of the total number of requests processed, 137 of them were submitted by federal law enforcement agencies in the conduct of terrorist financing investigations and 244 in the conduct of money laundering investigations. FinCEN also reported that 314(a) feedback from law enforcement requesters has been overwhelmingly positive. In approximately 2 years, February 2003 through March 2005, 314(a) requests submitted by law enforcement have resulted in the identification of thousands of new accounts and transactions. According to information that law enforcement provides to FinCEN, the 314(a) process has provided information that helped support the issuance of more than 800 subpoenas, 11 search warrants, and 9 arrests. However, FinCEN officials cautioned that this information represents feedback from only 10 percent of the cases for which 314(a) information requests were made and that FinCEN does not verify the accuracy of the data provided by law enforcement officials.

Almost all of the law enforcement officials we interviewed said that the 314(a) process improved the speed and efficiency of investigations by allowing investigators to query a large number of financial institutions in a short amount of time. One FBI official we interviewed showed us information on how a 314(a) request led to identification of additional suspect accounts across 23 states and 45 financial institutions. Prior to submitting the request, the FBI was aware of only four accounts. One law enforcement official told us that prior to section 314, law enforcement officials often sent subpoenas to individual banks for information. They could not, however, simultaneously request financial institutions across the country to search accounts or transactions for groups of individuals or even one person. According to FBI officials, the 314(a) process improves the efficiency of investigations because agents spend less time finding the suspect's specific financial transactions or accounts. The results from a 314(a) request may also help law enforcement to eliminate false leads. One prosecutor told us that the 314(a) process had been used 3 or 4 times during investigations of terrorist financing or money laundering cases. However, all of the law enforcement officials we interviewed told us that they are very judicious in their use of 314(a) requests, in part, because they were aware of the costs to the financial services industry and also because submitting the request can expose a covert operation. For instance, it is possible that a financial institution will take some action, permissible under the law, but which has the unintended effect of compromising the investigation.⁴⁴

According to some law enforcement officials, the 314(a) process also allows investigators to track down sophisticated criminals who might normally elude typical investigative approaches. For example, one prosecutor told us that a potential money launderer or terrorist financier with a lot of knowledge and sophistication about financial institutions might have been able to circumvent traditional approaches used to collect information, such as surveillance or tracing financial transactions to individual financial institutions. However, in her view, the 314(a) process has allowed investigators to cast a wider net thereby significantly improving the investigative effort.

⁴⁴Requests for information submitted by FinCEN to financial institutions pursuant to the rules adopted under 314(a) are confidential; however, financial institutions may use information provided by a section 314(a) request to determine whether to establish or maintain an account, or to engage in a transaction or to assist the financial institution in complying with the requirements of the BSA and the BSA Regulations.

Information Collected through CIP Can Assist Money Laundering and Terrorist Financing Investigations

Many of the law enforcement officials we interviewed said financial institutions are collecting and maintaining better and more detailed information as a result of CIP requirements. One prosecutor told us that as a result of section 326 regulations, grand jury subpoenas can be used to obtain more substantive and detailed information on accounts. This improvement was due to the fact that the CIP rule requires financial institutions to consistently gather more information from a customer when an account is opened. For example, investigators and prosecutors are now able to receive social security numbers, dates of birth, and complete addresses when they issue subpoenas. The same prosecutor told us that in the past, subpoenaed account information concerning criminal suspects was often incomplete. For instance, instead of a physical address they would receive only a P.O. Box or mailbox associated with the account. Standardization of account opening procedures has also made it easier for law enforcement to make positive matches with suspects on 314(a) lists. Prior to the enactment of the PATRIOT Act, some financial institutions already had established policies and procedures to verify customer identities, but the financial services industry overall was not subject to uniform minimum requirements for identifying and maintaining customer information. As a result, law enforcement officials did not always know what kind of information they would acquire from institutions pursuant to a subpoena or warrant.⁴⁵

Successful Prosecutions of Terrorist Financing and Money Laundering Cases Depend on Numerous Factors

Although the CIP requirement and 314(a) requests have made useful information available to federal prosecutors who are investigating and prosecuting terrorist financing and money laundering cases, prosecution of specific cases is always discretionary. Department of Justice officials, including prosecutors in U.S. Attorneys Offices, said that case specific factors continue to determine whether or not a prosecutor will bring charges on a terrorist financing or money laundering case. There are no specific monetary thresholds or criteria that determine when a prosecutor will pursue a money laundering or terrorist financing case. One prosecutor

⁴⁵See, for example: 31 U.S.C. 5318(h) and the regulations adopted pursuant thereto, which require certain financial institutions to adopt an anti-money laundering program that includes policies and procedures for verifying customer identity; 12 U.S.C. 1829b(c) and the regulations adopted pursuant thereto, which require certain financial institutions to maintain records and other evidence of customer identities; and 12 U.S.C. 1818(s) and the regulations adopted pursuant thereto, which require certain financial institutions to establish BSA compliance programs.

told us that these provisions helped prosecutors better understand the financial lay of the land in anti-money laundering and terrorist financing and that the use of the provisions by law enforcement leads to better investigations. It is not feasible, however, to enumerate how many cases were successfully prosecuted as a direct result of Suspicious Activity Reports or 314(a) requests since each prosecution is unique and based on many factors.

Prosecutors in two U.S. Attorney's Offices also told us that the provisions, while helpful, could not alter the fact that anti-money laundering and terrorist financing cases are resource intensive and complex. Prosecutors told us that reviewing transactions for a typical money services business or currency exchange was time consuming and may typically involve review of voluminous daily transaction records. Once the transaction analysis is performed, the information then must be reviewed in coordination with other evidence to determine if it can support proof beyond a reasonable doubt, and whether the evidence used to build the case is suitable for presentation in court.

Conclusions

Since the passage of the PATRIOT Act, the U.S. government and the financial industry have worked together to develop and implement the regulations required by the PATRIOT Act. It was challenging to develop joint regulations that covered so many sectors of the financial industry. The financial industry has implemented procedures to comply with the PATRIOT Act's regulations, including the CIP requirement and the information sharing provisions in section 314, but it has encountered several challenges along the way and there are some concerns and issues that remain outstanding. FinCEN, the federal financial regulators, and SROs have made a concerted effort to reach out to and educate the industry on its responsibilities for customer identification and sharing information with law enforcement. However, the interagency process has delayed the release of additional guidance for CIP. The implementation challenges that industry officials shared with us demonstrate that the government will need to continue its education efforts and work with industry to resolve outstanding issues. Primarily, industry officials are unclear about the regulators' views on what constitutes sufficient verification procedures for certain high-risk customers, such as foreign individuals and companies and whether they and their examiners would view a customer and the appropriate level of verification in the same way. Therefore, industry officials would like to receive more guidance from FinCEN and the regulators on issues such as these.

FinCEN, the federal financial regulators, and SROs have also taken steps to implement section 314 and CIP and have begun examining financial institutions and taking enforcement action for violations. However, our review revealed examiner difficulties in assessing compliance with CIP that could reduce its effectiveness at uncovering suspicious or questionable customers or lead to inconsistencies in the way examiners conduct examinations. Because our review found that not all examinations documented a review of the risk-based aspect of CIP, we believe that some examiners and financial institutions may not fully understand how the CIP requirements should be applied to higher risk customers. The primary reason that Treasury and the federal financial regulators adopted the risk-based approach to verifying customer identity was so that financial institutions would be able to focus more effort on high-risk customers. Also, some of the other difficulties we found in our review of examinations highlight how inconsistent interpretations can occur during examinations. For example, some examiners came to different conclusions about how the CIP requirement is applied to existing customers that open new accounts. Because examination findings can cause a financial institution to change its practices, such inconsistencies could lead to significant variations in policies and procedures among financial institutions based on differing interpretations of the CIP requirements by examiners.

Although our review focused on two specific anti-money laundering regulations, the enforcement of these regulations occurs under the broader BSA regulatory structure and, hence, the results of our review should be understood in this broader context. Enforcing the BSA, as amended by the PATRIOT Act, is a shared responsibility among FinCEN and the federal financial regulators. As the administrator of BSA, FinCEN has responsibility for enforcement of the provisions added by the PATRIOT Act, but FinCEN relies on the federal financial regulators to conduct examinations and alert it to violations that warrant an enforcement action. This arrangement is even more complicated for securities and futures financial institutions because SEC and CFTC largely rely on the SROs to conduct examinations and enforce rules and regulations. Since the passage of the PATRIOT Act, FinCEN and the financial regulators have been working more closely together to better coordinate BSA examinations and enforcement and to improve the consistency of the information they provide to the financial industry. FinCEN's new Office of Compliance and MOU with the federal banking regulators are good first steps in better BSA oversight and enforcement. In addition, FinCEN and the federal banking regulators have worked together to develop interagency anti-money laundering examination procedures for the first time. FinCEN is in the

process of reaching similar MOU agreements with SEC and CFTC. Whether in issuing guidance for industry or examiners, FinCEN will need the continued cooperation of all seven financial regulators to effectively address problems and inconsistencies in the U.S. anti-money laundering regulatory system.

Recommendations for Executive Action

To improve implementation of sections 326 and 314 of the PATRIOT Act, we are making two recommendations:

- To build on education and outreach efforts and help financial institutions subject to the CIP requirement effectively implement their programs, we recommend that the Secretary of the Treasury, through FinCEN and in coordination with the federal financial regulators and SROs, develop additional guidance covering ongoing implementation issues related to the CIP requirement. Specifically, additional guidance on the CIP requirement that provides examples or alternatives of how to verify the identity of high-risk customers, such as foreign individuals and companies, could help financial institutions develop better risk-based procedures.
- To enhance examination guidance covering the CIP requirement and ensure that examiners are well-informed about CIP requirements, we recommend that the Director of FinCEN work with the federal financial regulators to develop additional guidance for examiners to use in conducting BSA examinations. Specifically, the guidance should clarify that complying with the CIP requirement is more than determining whether the minimum customer identification information has been obtained—the examiner should determine whether a financial institution’s CIP contains effective risk-based procedures for verifying the identity of customers. Secondly, the guidance should clarify how CIP fits into other customer due diligence practices, such as know-your-customer procedures. Finally, the guidance should reflect the FAQs on CIP issued for industry, which addressed the difficulties in interpretation we observed for checking government lists and applying the CIP requirement to existing customers.

Agency Comments and Our Evaluation

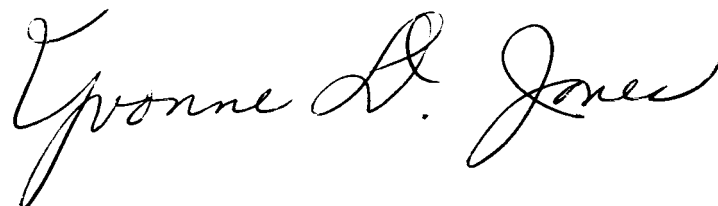
We provided a draft of this report for review and comment to the Departments of the Treasury, Justice, and Homeland Security; seven federal financial regulators (Federal Reserve, FDIC, OCC, OTS, NCUA,

SEC, and CFTC) and five SROs (CBOT, CME, NFA, NASD, and NYSE). We received written comments from the Department of the Treasury, NCUA, and SEC. These comments are reprinted in appendixes II, III, and IV. The Departments of the Treasury and Justice, the Federal Reserve, FDIC, OCC, SEC, CFTC, NASD, NYSE and NFA also provided technical comments and clarifications, which we incorporated in this report where appropriate. The Department of Homeland Security, OTS, CME, and CBOT had no comments.

In its written comments, Treasury said that despite the considerable educational and outreach efforts already undertaken by FinCEN, there was still some confusion and lack of clarity on the part of both the federal financial regulators and SROs, and the regulated industries and examiners who conduct compliance inspections of these industries. Treasury concurred with our recommendations that additional guidance would improve implementation of these regulations. Treasury also commented that, with the diversity of financial institutions that must comply with CIP regulations, firms need the flexibility to implement programs tailored to their own size, location, and type of business and to allow them to use a risk-based approach to verify the identity of their respective customer bases. In its written comments, NCUA also supported our recommendations. Both agencies commented that Treasury and the federal banking regulators plan to issue new BSA examination procedures in June 2005. In its written response, SEC commented that consistent with our recommendation, the federal financial regulators are continuing to work cooperatively to ensure that they provide consistent guidance on interpretive and compliance issues. Concerning difficulties SEC had with its examination tracking system when responding to our information request, SEC also said that its staff is formulating improvements to the existing automated tracking system.

Unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this report. At that time, we will send copies of this report to the Departments of the Treasury, Homeland Security, and Justice; the Federal Reserve Board, FDIC, OCC, OTS, NCUA, CFTC, SEC, NASD, NYSE, NFA, CBOT, CME, and interested congressional committees. We will also make copies available to others on request. In addition, this report will be available at no cost on our Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report please contact me at (202) 512-2717 or Barbara Keller, Assistant Director, at (202) 512-9624. GAO contacts and key contributors to this report are listed in appendix V.

A handwritten signature in black ink that reads "Yvonne D. Jones". The signature is written in a cursive style with a large initial 'Y' and a distinct 'D'.

Yvonne D. Jones
Director, Financial Markets and
Community Investment

Scope and Methodology

To determine how Treasury and the federal financial regulators developed the regulations for CIP and section 314 and identify challenges, we reviewed documents related to the rulemaking process including comment letters and the *Federal Register* notices of the final rules and interviewed officials from Treasury (FinCEN), Justice, the federal financial regulators, and SROs.

To identify the government's education and outreach efforts, we interviewed officials from Treasury (FinCEN), the federal financial regulators, and SROs about how they have informed and educated the industry and reviewed education and outreach materials provided to us. To identify implementation challenges encountered by financial institutions, we interviewed company officials and industry trade associations representing banks, credit unions, securities broker-dealers, mutual funds, futures commission merchants, and futures introducing brokers. We also reviewed letters that company officials and industry representatives sent to Treasury and the federal financial regulators during the rulemaking process as well as after the final rules were issued that expressed concerns and challenges they had about implementing procedures to comply with CIP and section 314 regulations.

To determine the extent to which the federal financial regulators and SROs have updated examination guidance and trained examiners on CIP and section 314, we reviewed copies of draft and final versions of guidance; collected information on examiner training courses related to anti-money laundering and the number of examiners trained in 2002, 2003, and 2004; and interviewed officials on their examination guidance and training programs. We also observed one anti-money laundering training course taught by the Federal Financial Institutions Examination Council (FFIEC) that provides training to bank examiners.

To determine the extent to which the federal financial regulators have examined for compliance and taken enforcement actions on CIP and section 314 regulations, we collected data on the number of exams completed from October 1, 2003, through May 31, 2004, and the number of violations for CIP and section 314 regulations for the same time period from six federal financial regulators and five SROs. The data from the regulators and SROs generally came from information systems and reporting processes used to collect and track information on examinations and violations. There was some variability in how the regulators and SROs defined examinations, violations, and the start and end dates for examinations and therefore the data are not comparable. However, we

determined that the data provided to us were generally reliable for our purposes. Our data reliability assessments generally involved interviewing officials about the management of the data and basic tests of the data to determine if it appeared accurate. We attempted to select approximately 20 examinations from each regulator and SRO. To ensure that we would be able to review a sufficient number of examinations with the types of violations related to CIP and section 314 requirements and how the regulators and SROs addressed violations, we sampled proportionally more examinations that included violations of CIP and section 314 than examinations without violations, though in some cases the number of examinations that had such violations were less than 10 and, therefore, the sample would not include proportionally more examinations with violations. We reviewed a total of 176 examinations. However, the number of examinations varied widely between organizations, and in the cases of CBOT and CME, all available examinations were selected because the number of examinations was small.¹ While the selections of individual examinations were made randomly within the subsets of violation and nonviolation examinations to minimize the possibility of bias in our sample, the arbitrary totals selected were small in number and not representative of the true ratio of violation to nonviolation examinations within the organization nor the volume of examination activity across the organizations. Therefore, these samples are not statistically representative. However, our review of the examinations enabled us to describe the approaches used by the regulators to examine for compliance and highlight issues that may present challenges for examiners in interpreting the new regulations and appropriately assessing financial institutions for compliance. Table 11 displays the final sample size for each of the regulators and SROs and also explains why some examinations initially selected were not part of our final sample.

¹The samples for CBOT and CME encompass all of the examinations that included anti-money laundering compliance completed between October 1, 2003, and May 31, 2004. The futures exchanges began anti-money laundering examinations in 2002 and plan to reexamine firms for anti-money laundering compliance approximately every 3 examination cycles, which ranges from 9 to 18 months, unless they are conducting an examination to follow-up on deficiencies. Therefore, during our review period, the only examinations CBOT and CME conducted were follow-up examinations.

**Appendix I
Scope and Methodology**

Table 11: Description of Our Approach for Sampling Examinations Covering CIP and Section 314

Regulator or SRO	Population of examinations from which we sampled^a	Number of exams initially sampled	Number of exams in final sample	Number of examinations with no violations of CIP or section 314	Number of examinations with violations of CIP and/or section 314
FDIC	1,333	20	20	7	13
Federal Reserve	414	20	20	8	12
NCUA	2,109	20	20	8	12
OCC—small & mid-size banks	39	16	16	12	4
OCC—large banks	9	4	4	3	1
OTS ^b	245	20	16	9	7
SEC-Broker Dealers	26	11	11	5	6
SEC—Mutual Funds ^c	71	11	6	6	0
NASD	654	20	20	5	15
NYSE	86	21	21	15	6
NFA ^d	193	20	18	5	13
CME	2	2	2	1	1
CBOT	2	2	2	2	0

Source: GAO analysis and samples of regulator and SRO data.

^aThe population of examinations from which we pulled our sample should not be interpreted as the total number of examinations covering anti-money laundering compliance during this time period. Rather, the population generally represents the examinations identified by the regulator or SRO as more likely to cover section 314 and CIP. We also deleted some examinations provided to us in the original data sets because they fell outside our timeframes or were ineligible for our purposes (e.g., examinations conducted by a state regulator).

^bThe original OTS sample mistakenly had 3 duplicate exams in the violation sample. An additional exam was dropped at OTS request because an examiner needed the workpapers for a follow-up exam. Therefore, the OTS sample changed from 20 examinations to 16 exams.

^cOur initial sample of mutual funds was based on data provided by SEC that included examinations of transfer agents in which anti-money laundering compliance was not required to be a part of the examination. Therefore, we had to drop four transfer agents that we had initially selected in our sample. Also, our sample of mutual funds picked up a Unit Investment Trust, which is not subject to anti-money laundering rules at this time and so we dropped it from our sample. Overall, the original sample of 11 mutual fund entities was reduced to 6.

^dTwo examinations in the NFA sample were dropped because one firm was withdrawing its registration and the other examination was a limited scope exam on the firm's financial position; therefore, these examinations should not have been in the sample.

After selecting our sample of examinations, we requested the examination reports and related workpapers associated with each examination from each of the regulators and SROs. We developed a data collection instrument to review the examination documentation. The data collection

instrument was developed by reviewing the regulation requirements for CIP and section 314 and the examination procedures developed by the regulators and SROs. After each examination was reviewed once using the data collection instrument, a second person reviewed the examination using the data collection instrument a second time to ensure the reliability of our coding of the review questions and accuracy of data entry. We used the results from the data collection instrument to determine how the regulators and SROs reviewed compliance and how regulators and SROs dealt with deficiencies and violations related to CIP and section 314. We also identified formal enforcement actions that were completed during the time of our review and included violations of CIP or section 314 regulations. Finally, we interviewed officials from FinCEN, the federal financial regulators, and SROs about their examination and enforcement policies.

To determine how these new regulations have and could improve law enforcement investigations and prosecutions of money laundering and terrorist activities, we interviewed officials representing several law enforcement agencies, including the FBI and ICE, and Department of Justice officials. We interviewed supervisory prosecutors from two U.S. Attorneys offices as well as supervisory officials at the Asset Forfeiture and Money Laundering Section and the Counter-Terrorism Section at the Department of Justice who have been involved with money laundering and terrorist cases and had experience with section 314 and CIP to better understand the factors that are considered when deciding whether to prosecute a money laundering or terrorist financing case. We also reviewed information that FinCEN collects from law enforcement agencies on the results of the 314(a) process.

We conducted our work in New York City, NY; Chicago, IL; and Washington, D.C., between February 2004 and March 2005 in accordance with generally accepted government auditing standards.

Comments from the Department of the Treasury



UNDER SECRETARY

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

May 2, 2005

Ms. Yvonne D. Jones
Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Jones:

I am writing to provide the Department of the Treasury's comments on the draft report entitled, USA PATRIOT Act – *Additional Guidance Could Improve Implementation of Regulations Related to Customer Identification and Information Sharing Procedures*. The report was a review of the implementation of two provisions of the USA PATRIOT Act -- Sections 314 and 326 -- and it contains two recommendations: (1) FinCEN, in consultation with the federal financial regulators and SROs, needs to develop additional guidance for industry on ongoing implementation issues and (2) FinCEN needs to develop additional guidance for examiners to improve the quality and consistency of examinations of the customer identification program (CIP) requirement.

With regard to both recommendations, the Department of the Treasury concurs with the findings of the report that additional guidance would improve implementation of these regulations. We understand that despite the considerable education and outreach already undertaken by FinCEN, there still exists some confusion on the part the federal financial regulators and SROs, the regulated industries, and the examiners who conduct compliance inspections of these industries. FinCEN is committed to publishing additional guidance and becoming more involved in helping the federal financial regulators develop examination guidance and best practices. Moreover, whether in issuing guidance for industry or examiners, FinCEN will continue to cooperate with the financial regulators to effectively address problems and inconsistencies in the U.S. anti-money laundering regulatory system.

On April 28, 2005, FinCEN issued a new set of inter-agency Qs&As on Section 326 that we believe will address a number of areas of concern. In addition, through its participation with the Federal Financial Institutions Examination Council, FinCEN is working closely with the federal banking agencies to develop new uniform examination procedures and guidelines to better ensure consistency in Bank Secrecy Act compliance examination procedures. These new procedures are expected to be issued in June of this year. In addition, FinCEN signed Memoranda of Understanding with the federal banking agencies, the IRS, and the New York State Banking Department, and they expect to have several additional MOUs with other States in the coming months. Through the execution

Appendix II
Comments from the Department of the
Treasury

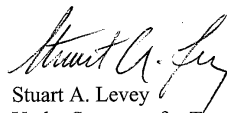
of such information sharing agreements, I am confident that consistency in the application of the Bank Secrecy Act will be better achieved.

I would like to make one additional comment regarding the risk-based aspect of CIP, which was noted in the report as an area that could be difficult for both financial institutions and examiners to interpret consistently. The report stated that determining the level of risk of a customer or account can be difficult and depends on several factors, such as the customer's line of business, the process used to open the account, and whether the customer is in the United States or overseas. While we agree with the report's assessment, we believe that it was essential to adopt a risk-based approach. Given the diversity of financial institutions that must comply with these regulations, we believe that firms need the flexibility to implement programs tailored to their own size, location and type of business and to allow them to use a risk-based approach to verify the identity of their respective customer bases.

In addition, I would like to request that on page 46 of the report, the section entitled, CIP Requirements for Checking Government Lists, the following sentence be changed to read as follows: "However, as FinCEN and the banking regulators noted in the first set of CIP FAQs, lists published by OFAC whose independent requirements stem from statutes other than the USA PATRIOT Act and are not limited to terrorism, have not been designated for purposes of the CIP rule."

Thank you for the opportunity to respond to this report on the USA PATRIOT Act. If you have any questions or wish to discuss these comments further, please contact FinCEN's Associate Director, William Langford, at 202-354-6414.

Sincerely,



Stuart A. Levey
Under Secretary for Terrorism & Financial Intelligence

Cc: Juan C. Zarate, Assistant Secretary, Terrorist Financing & Financial Crime;
William J. Fox, Director, FinCEN

Comments from the National Credit Union Administration



National Credit Union Administration

April 26, 2005

Yvonne Jones, Director
Government Accountability Office
Financial Markets and Community Investment
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Jones:

We have reviewed your draft report entitled USA Patriot Act: Additional Guidance could Improve Implementation of Regulations Related to Customer Identification and Information Sharing Procedures (GAO 05-412).

The National Credit Union Administration (NCUA) supports your recommendations to provide additional guidance concerning the implementation of Customer Identification Programs (CIP) required by the USA Patriot Act.

In January 2004, the federal banking regulators¹, Financial Crimes Enforcement Network (FinCEN), and the United States Department of the Treasury published guidance in the form of Frequently Asked Questions (FAQs) addressing CIP. A second set of FAQs will be published during 2005.

In June 2005, the federal banking regulators plan to publish examination procedures for compliance with the Bank Secrecy Act. The procedures address CIP concepts, including risk assessment and due diligence practices. While FinCEN contributed to these procedures, NCUA anticipates the procedures will be finalized and published by the Federal Financial Institutions Examination Council².

Thank you for the opportunity to review and comment on your report.

Sincerely,

A handwritten signature in cursive script that reads 'JoAnn Johnson'.

JoAnn Johnson
Chairman
National Credit Union Administration

EI/EAH:eah

¹ The federal banking regulators include the National Credit Union Administration, Board of Governors of the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

² The Federal Financial Institutions Examination Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision and to make recommendations to promote uniformity in the supervision of financial institutions.

1775 Duke Street - Alexandria, VA 22314-3428 - 703-518-6300 - 703-518-6319 FAX

Comments from the Securities and Exchange Commission



OFFICE OF COMPLIANCE
INSPECTIONS AND
EXAMINATIONS

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

April 25, 2005

Yvonne D. Jones
Director
Financial Markets and Community Investment
United States Government Accountability Office
Washington, D.C. 20548

Re: USA PATRIOT Act: Additional Guidance Could Improve Implementation of Regulations Related to Customer Identification and Information Sharing Procedures (GAO-05-412)

Dear Ms. Jones:

Thank you for the opportunity to comment on the Government Accountability Office's (GAO) draft report entitled USA PATRIOT Act: Additional Guidance Could Improve Implementation of Regulations Related to Customer Identification and Information Sharing Procedures.

As you know, the federal financial regulators worked together with FinCEN to develop a series of customer identification rules that apply equally to different financial institutions, while also taking into account the institutions' different business models and customer relationships. By creating minimum standards for collecting identifying information, these rules have helped ensure that firms can obtain the information they need to fulfill their obligations under the rules implementing Section 326. Consistent with GAO's recommendation, the federal financial regulators are continuing to work cooperatively to ensure that they provide consistent guidance on interpretive and compliance issues. In addition, the SEC staff regularly works with other regulators on anti-money laundering issues, including with FinCEN and the securities self-regulatory organizations (SROs), as well as with securities industry representatives.

As the GAO report illustrates, the SEC is committed to its anti-money laundering examination program. The examination staff launched its anti-money laundering initiative with respect to broker-dealers in advance of the enactment of the USA PATRIOT Act, and began reviewing certain aspects of mutual funds' customer identification programs in advance of the adoption of final customer information program rules for mutual funds. This provided both examiners and the industry advanced opportunity to acclimate to the new requirements. The current examination program includes the review of broker-dealers' and mutual funds' customer information and information sharing programs, as well as oversight of the SROs' anti-money laundering examinations of broker-dealers. The GAO report highlighted the importance of the

Appendix IV
Comments from the Securities and Exchange
Commission

Yvonne D. Jones
April 25, 2005
Page 2 of 2

ability to track examinations and their results. The SEC staff uses both an exam tracking system and a database of examination reports, which are designed to complement each other. The SEC's technology staff is formulating improvements to the existing automated tracking system.

Anti-money laundering examinations continue to be a cooperative process. The SEC staff conducts joint training sessions with the SROs, in which FinCEN participates. The SEC staff also meets regularly with the SROs and FinCEN to discuss new developments. In addition, the SEC and FinCEN have been discussing methods to share information more routinely.

Thank you and your staff for your courtesy during this review.

Sincerely,



Lori A. Richards
Director

GAO Contacts and Staff Acknowledgments

GAO Contacts

Barbara I. Keller (202) 512-9624
Kay D. Kuhlman (202) 512-2755

Staff Acknowledgments

William Bates, Davi M. D'Agostino, David Nicholson, Carl Ramirez, Omyra Ramsingh, Adam Shapiro, and Kaya Leigh Taylor made key contributions to this report.

Related Products

Anti-Money Laundering: Issues Concerning Depository Institution Regulatory Oversight. [GAO-04-833T](#). Washington, D.C.: June 3, 2004.

Combating Money Laundering: Opportunities Exist to Improve the National Strategy. [GAO-03-813](#). Washington, D.C.: September 26, 2003.

Internet Gambling: An Overview of the Issues. [GAO-03-89](#). Washington, D.C.: December 2, 2002.

Interim Report on Internet Gambling. [GAO-02-1101R](#). Washington, D.C.: September 23, 2002.

Money Laundering: Extent of Money Laundering through Credit Cards is Unknown. [GAO-02-670](#). Washington, D.C.: July 22, 2002.

Anti-Money Laundering: Efforts in the Securities Industry. [GAO-02-111](#). Washington, D.C.: October 10, 2001.

Money Laundering: Oversight of Suspicious Activity Reporting at Bank-Affiliated Broker-Dealers Ceased. [GAO-01-474](#). Washington, D.C.: March 22, 2001.

Suspicious Banking Activities: Possible Money Laundering by U.S. Corporations Formed for Russian Entities. [GAO-01-120](#). Washington, D.C.: October 31, 2000.

Money Laundering: Observations on Private Banking and Related Oversight of Selected Offshore Jurisdictions. [GAO/T-GGD-00-32](#). Washington, D.C.: November 9, 1999.

Private Banking: Raul Salinas, Citibank, and Alleged Money Laundering. [GAO/T-OSI-00-3](#). Washington, D.C.: November 9, 1999.

Private Banking: Raul Salinas, Citibank, and Alleged Money Laundering. [GAO/OSI-99-1](#). Washington, D.C.: October 30, 1998.

Money Laundering: Regulatory Oversight of Offshore Private Banking Activities. [GAO/GGD-98-154](#). Washington, D.C.: June 29, 1998.

Money Laundering: FinCEN's Law Enforcement Support Role Is Evolving. [GAO/GGD-98-117](#). Washington, D.C.: June 19, 1998.

Related Products

Money Laundering: FinCEN Needs to Better Manage Bank Secrecy Act Civil Penalties. [GAO/GGD-98-108](#). Washington, D.C.: June 15, 1998.

Money Laundering: FinCEN's Law Enforcement Support, Regulatory, and International Roles. [GAO/GGD-98-83](#). Washington, D.C.: April 1, 1998.

Money Laundering: FinCEN Needs to Better Communicate Regulatory Priorities and Timelines. [GAO/GGD-98-18](#). Washington, D.C.: February 6, 1998.

Private Banking: Information on Private Banking and Its Vulnerability to Money Laundering. [GAO/GGD-98-19R](#). Washington, D.C.: October 30, 1997.

Money Laundering: A Framework for Understanding U.S. Efforts Overseas. [GAO/GGD-96-105](#). Washington, D.C.: May 24, 1996.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548