

Update For Federally Regulated "Banks" Regarding USA PATRIOT ACT Customer Identification Program

In May 2003 the Department of the Treasury, acting through several federal regulators pursuant to the USA PATRIOT Act, published final rules requiring certain financial institutions to develop a Customer Identification Program (CIP) to minimize the risk and detect and prevent money laundering and financing of terrorism. The regulations required implementation of a Customer Identification Program by **October 1, 2003** which should include procedures for verifying the identity of any prospective customer (including policies for opening or refusing to open accounts in light of identity verification); maintaining records of the information used for identity verification; and consulting lists of known or suspected terrorists or terrorist organizations to determine whether the prospective customer appears on any such list. For additional information on the specific requirements of these regulations, see <http://www.mckennalong.com/attachment.html/articles/914/Customer+Identification+Program+Rules.pdf>. This advisory will (1) review recent guidance regarding these regulations and (2) provide practical considerations for federally regulated "banks."

In This Issue:

- [Recent Guidance Regarding Regulations](#)
- [Practical Considerations for Federally Regulated "Banks"](#)

Recent Guidance Regarding Regulations

In January of 2004, federal bank regulators and the United States Department of the Treasury, in a joint release, issued FAQs: Final CIP Rule, to provide interpretative guidance regarding the rules implemented, effective October 1, 2003. In wide ranging series of questions and answers, the agencies provide guidance in connection with questions that have emerged since the effective date of the CIP final rules. It is suggested that the Compliance Officer or the person or group charged with implementation and oversight of the CIP carefully study the FAQs provided by the agencies and along with the basic principles set forth in the CIP rules, perform a risk based analysis for the program in effect for verifying the identity of each customer. With the regulations in place, examination procedures will be the focus in 2004, with examiners focusing on anti-money laundering procedures and policies for compliance with suspicious activity reports. It also appears that the OFAC is implementing examination procedures with a view toward examination of bank systems, policies and procedures that are in place in order to detect and avoid illegal transfers of funds. It is also expected that in 2004 the Department of Homeland Security will focus on money laundering and Patriot Act issues.

On October 20, 2003, federal bank and thrift regulators issued examination procedures targeting the Treasury regulations issued under the USA PATRIOT Act.

Contact Info

If you would like more information, please contact any of the McKenna Long & Aldridge attorneys with whom you regularly work. You may also contact:

William L. Floyd
404.527.4010

Trey Wainwright
404.527.4659

The new procedures require a detailed review of Bank Secrecy Act and anti-money laundering procedures and examination of required recording keeping. The specific examination procedures require an examiner to review the following: (i) policies and procedures for responding to FinCEN requests; (ii) handling of positive matches; (iii) methods for keeping information secure and confidential; (iv) filing of SARs; and (v) documentation of compliance. The new procedures also focus on examination of all foreign bank correspondent accounts and related records to ensure that financial institutions are not maintaining correspondent accounts with or for foreign shell banks that maintain no physical presence in any country.

In a similar move, the Federal Deposit Insurance Corporation issued new procedures for its examiners to assess compliance with the anti-money laundering program of financial institutions based on requirements of the Bank Secrecy Act. The new procedures follow a question and answer format designed to address risk management and anti-laundering strategies for each of the bank's major business activities. According to the FDIC, the new examination procedures will be in effect for all safety and soundness examinations. Where the financial institution is deemed to engage in high risk activities, such as transactions with offshore companies, transactions over the Internet, high volume customers with frequent use of overdraft protection, significant deposits of cash and frequent wire transfers, and the like, expanded procedures will be used, with more detailed compliance checks.

As an example of heightened scrutiny in the examination process, recently, the Federal Reserve Bank of Richmond and the banking commissioner of North Carolina entered into a written supervisory agreement with a bank in Charlotte, North Carolina specifically dealing with anti-money laundering programs. The following were major points covered by the written agreement:

- The anti-money laundering program is required to include procedures which on a continuing basis, identify and incorporate the requirements of any and all amendments to the Bank Secrecy Act, together with internal control procedures designed to ensure compliance.
- Establish a written program for conducting "Customer Due Diligence" and to identify and report any and all suspicious activities, including a risk based assessment of the bank's customer base with a special program implemented for categories of customers believed to pose a heightened risk.
- Implement specific procedures and "enhanced due diligence" for customers that are categorized to pose a heightened risk.

The more specific portions of the written agreement involving compliance with the Bank Secrecy Act and anti-money laundering programs were tied directly to the CIP program implemented by the bank.

In addition to the examiners' focus on matters covered by the USA PATRIOT Act, the Office of Foreign Assets Control has recently announced fines assessed against several New York based banks, each of which had voluntarily disclosed violations of requirements of the Office of Foreign Assets Control, and all of which related to funds transfers involving Libya and Cuba, two of the "sanctioned countries" on OFAC's restricted list.

Practical Considerations for Federally Regulated "Banks"

▶ Implementation; Penalties

Management should remember that the institution will be reviewed for compliance with both the regulations and the policy adopted. Adoption of a policy that is fully compliant with the regulations and requirements is only the first step. Failure to follow the policy will be considered a violation of the requirements of the statute and applicable regulations. Penalties for violation of the CIP identity verification and reporting requirements may include significant fines for both the institution and the individual employee, and possibly imprisonment. Accordingly, diligent training programs must be developed and periodically updated in order to make certain that all employees involved in this process understand their responsibilities.

▶ Relevant Risks

Each covered institution must analyze its business and business strategy in order to assess the operational risks for money laundering. For example, high end private banking services may pose greater risks than traditional consumer accounts. Correspondent accounts with foreign financial institutions could pose risk as could foreign customers, depending upon the country of origin and related considerations. Additional risk-based standards should be considered for businesses involving accounts or transactions that are opened or performed without any face-to-face contact. If the processes and procedures established by the institution do not require cross reference with government designated lists prior to opening an account, the institution should provide the customer notice that the account is still subject to identity verification and may be suspended or closed if a question occurs. Much as was the case in complying with filing of Suspicious Activity Reports, the customer identification policy and procedure should include a system for prompt notification of federal regulatory authorities where appropriate.

▶ Privacy Issues

It is very important that the policies and procedures developed are viewed in light of the privacy requirements under the Gramm-Leach-Bliley Act and the privacy policy adopted by the institution. Also, the actual privacy notice sent to customers should be reviewed to ensure compatibility with the Customer Identification Program, specifically, whether this information can be shared with other institutions and, if so, whether the legal obligations under the Right to Financial Privacy Act have been observed.

It should be noted that on December 30, 2003, an interagency proposal was issued under the Gramm-Leach-Bliley Act which would allow alternative forms of privacy notice that would be easier for consumers to understand. The interagency proposal seeks comments by March 29, 2004 on a wide ranging series of issues dealing with the efficacy of privacy notices. Any modification to regulations issued under Gramm-Leach-Bliley likely will take some time given the number of agencies involved in the request for comments. There are also several pending legislative actions dealing with financial privacy, with several bills pending in the House and Senate. Given the recent legislative action amending the Fair Credit Reporting Act, it does not seem likely that pending legislation involving financial privacy soon will be enacted.

▶ Outsourcing Arrangements

In order to assure compliance with the Customer Identification Program, an institution also should review its current agreements with data processing providers and other service providers to make certain that outsourced functions comply with the Customer Identification Program implemented.

▶ Internal Oversight

The internal audit function of each institution should be modified and directed to provide an oversight of the Customer Identification Program as tied into the Bank Secrecy Act and anti-money laundering programs of the institution. That function should report its findings to either the Chief Compliance Officer or the Chief Legal Officer of the institution. We also recommend that information regarding the Customer Identification Program and its application should be the subject of a confidential anonymous reporting system where an employee can and is encouraged to anonymously report issues involving this program and application of the policy to a responsible authority, presumably the Chief Compliance Officer or directly to the Audit Committee.

▶ [Back to top](#)

■ About Us

McKenna Long & Aldridge LLP is a full-service law firm of approximately 375 lawyers and public policy advisors. The firm provides business solutions in the areas of corporate law, government contracts, intellectual property and technology, complex litigation, public policy and regulatory affairs, real estate, environmental, energy and finance.

■ Subscription Info

If you would like others to receive our future mailings, please email their contact information to us at information@mckennalong.com

If you would like to be removed from our Corporate Advisory mailing list, please email information@mckennalong.com

*This **Corporate Advisory** is for informational purposes only and does not constitute specific legal advice or opinions. Such advice and opinions are provided by the firm only upon engagement with respect to specific factual situations. This message is intended as a transactional message for clients of the Firm. If you are not a client of the Firm, you have received it for informational purposes only and should not consider it an advertisement or solicitation.

• Atlanta • Brussels • Denver • Los Angeles • Philadelphia • San Diego • San Francisco • Washington D.C.

©Copyright 2004, McKenna Long & Aldridge LLP, Suite 5300, 303 Peachtree Street, NE, Atlanta, GA 30308