



Office of Thrift Supervision
Department of the Treasury

1700 G Street, N.W., Washington, DC 20552 • (202) 906-6000

USA PATRIOT ACT PREPAREDNESS CHECK-UP

A Framework for Achieving Compliance with New USA PATRIOT Act Regulations

In issuing final regulatory requirements for Customer Identification Programs (CIP), Treasury and the banking agencies have established a compliance deadline of October 1, 2003. This affords thrifts the opportunity to evaluate their current practices and make necessary changes to assure compliance by the deadline. To assist you, we created this preparedness check-up to guide your efforts to achieve timely compliance. This framework should be useful in updating your current Bank Secrecy Act – Anti-Money Laundering (BSA/AML) program for other USA PATRIOT Act (USAPA) requirements in addition to the CIP rule, such as requirements related to responding to law enforcement information requests and to managing private banking accounts of non-U.S. persons.

We encourage all institutions to ADAPt their current BSA/AML program to the new USAPA requirements: **Analyze** their current program; **Develop** a comprehensive BSA/AML program, which includes a customer identification program that addresses all of the thrift's business lines; **Apply** your revised program throughout the affected day-to-day operations; and **Test** the new program through internal audits and testing to ensure that the program functions as intended.

ANALYZE: Review your current BSA/AML program and compare it to your business strategy, operational risks, and available resources. Ask the following questions:

- *How does the way we conduct our business expose us to risk from money laundering or terrorist financing activities?*
 - What are our current business lines and how do we generate our customers?
 - Do we offer private banking services? If so, do we maintain private banking accounts for non-U.S. citizens and do those accounts exceed \$ 1 million?
 - Do we maintain correspondent accounts for foreign financial institutions? If yes, what country of origin are the banks that maintain the account?
- *What are the practices we currently follow to assure the identity of our customers?*
 - What are our current policies for obtaining identifying information from our customers?
 - Do we currently verify the identification information that we obtain from our customers, and if so, how? When do we make exceptions to identity verification and why?

- Do we keep a record of the information we obtain and verify?
- What is our practice for sharing information with law enforcement or others about persons whose identity or conduct we suspect?
- *What means do we use to keep our procedures, our people and our service providers up to date with respect to BSA/AML compliance obligations?*
 - What types of BSA training do we provide to bank personnel and how has it kept pace with changes since September 11, 2001?
 - What systems do we rely on to comply with current BSA requirements? Have we purchased additional software/system support to comply with USAPA regulations?
 - In what ways do third party providers currently play a role in our BSA/AML program? Have the third party providers we use adjusted their systems to meet USAPA obligations?
 - When was the last time our board reviewed and approved our BSA/AML program?
 - What does our last internal audit tell us about our record of BSA/AML compliance and our ability to self-identify and self-correct program deficiencies before bank examiners find them?
 - Have we designated an individual to be in charge of overall BSA/AML compliance and afforded that person adequate authority and resources to do the job? Is our current staffing in the BSA area adequate given the responsibilities imposed by USAPA?
 - How well did we handle responding to the “Control List?” (CEO Memo 151.) What does that or other more recent experience tell us about our ability to receive and respond in a timely fashion to information requests generated by FinCEN pursuant to Section 314(a) or other government designated lists?

DVELOP: After analyzing your current policies, procedures, and risks, you will probably need to add to your already existing BSA/AML program in order to fully comply with the new USAPA regulations and other general regulatory requirements. Ask the following questions:

- *Have we addressed each of the regulatory requirements in devising our Customer Identification Program?*
 - Have we approached the development of our new program with industry “best practices” in mind?
 - Do the customer identification elements of our BSA/AML program adequately address all of our business lines and methods for generating accounts?
 - Does our CIP address how we will collect at least the minimum information required by the rule for persons opening accounts including name, appropriate address, date of birth (for individuals), and government issued identification number (such as a social security number)?

- Do we have products, services, or market segments that warrant collecting more than the minimum amount of information to enable us to adequately identify our customers, and if so, have we described those accounts or occasions that trigger additional information collection and the elements to be gathered?
- Does our CIP address how we will verify identification information to attain a reasonable belief regarding the true identity of our new customers or existing customers opening new accounts?
- Have we covered situations where accounts are opened without face-to-face contact?
- Does our CIP provide appropriate risk-based standards for assessing new accounts opened by a customer that is not an individual? Do those standards provide that in such cases the thrift will obtain information about other individuals with authority or control over an account, such as signatories, in order to verify the customer's identity?
- Does our CIP specify situations where we will not offer banking services, will permit a customer to have limited use of an account while verifying the customer's identity, or will actually close an account?
- Have we devised a prompt process to determine whether the customer appears on government designated lists of known or suspected terrorists?
- Have we drafted the required notice to customers advising them that we will verify their identity in accordance with our legal obligation and policies?
- Have we determined how customers will be notified about identity verification requirements?
- *Have we revised our BSA/AML program to address any business operations that require enhanced scrutiny?*
 - Have we developed standards for enhanced due diligence for our private banking accounts involving non-U.S. persons? Have we determined whether or under what circumstances this level of diligence should apply to similar accounts of U.S. persons? Is it clear from our revised program that enhanced due diligence applies to existing, and not just new, private banking accounts?
 - Have we developed standards for enhanced due diligence for our correspondent accounts with foreign banks that take into account the particular foreign institutions involved and the risk of improper activity attendant to the circumstances presented?
- *Have we devised a system for promptly responding to law enforcement inquiries and securely sharing customer information with other institutions?*
 - Does our program designate someone who is responsible for receiving and acting on law enforcement requests distributed pursuant to Section 314(a) of USAPA?
 - Is there a process to follow to promptly respond to law enforcement inquiries about persons suspected of money-laundering or terrorist financing?

- Have we decided whether and under what conditions to share information with other institutions about customers engaged in suspicious activities? Do those plans meet our legal obligations under the Right to Financial Privacy Act, GLBA and USAPA?
- *Have we charted a course to attain compliance in a timely fashion?*
 - Do responsibilities for OFAC compliance continue to be adequately covered after revisions to our BSA/AML program?
 - Will our updated BSA/AML program that includes the CIP be presented to, reviewed by and approved by the Board of Directors as part of the BSA compliance program in advance of the October 1, 2003 compliance deadline? Will the Board be sufficiently versed in USAPA issues and institution operations to take informed action on the updated program?
 - Are agreements with service providers being modified to include any changes necessary to assure they perform in accordance with our program and our regulatory obligations?
 - Are training modules being developed or acquired and employees being scheduled for training in accordance with their responsibilities?
 - Have we alerted internal audit or compliance review functions to the need to modify their oversight standards to cover the CIP and other changes in our BSA/AML program and regulatory obligations?

APPLY: After analyzing your current program and developing the necessary enhancements, thrifts must implement necessary changes in BSA policies and procedures. Ask the following questions:

- *Is staff informed of new requirements?*
 - What communications are being made to assure that all employees with a role in the CIP or BSA/AML are aware of their new program responsibilities or any changes in past responsibilities?
 - Have new approved policies and procedures been distributed to managers and staff?
 - Is staff training going according to plan?
 - Is the person coordinating implementation providing timely and accurate responses to staff questions and requests for guidance?
 - Is there a process for informing staff of further regulatory developments?
- *Are changes in customer identification information collection and verification practices occurring?*
 - Do we observe new customers receiving notices and providing requested identification?
 - Are any new forms being filled in completely and accurately?

- How are employees dealing with the reaction of existing customers opening new accounts?
- Are those responsible for verification of customer identities and comparison of names against designated government lists doing those tasks in the time frames called for by our CIP and regulatory standards?
- Does it appear that enough resources have been provided to sufficiently fulfill any increased compliance burden?
- Are the requisite records being maintained?
- *Are private banking accounts with non-U.S. persons and any foreign bank correspondent accounts being handled appropriately?*
 - Did we conduct a thorough review of our private banking and correspondent accounts to identify those that are subject to our program's enhanced due diligence?
 - Do the findings resulting from our account review warrant taking action to close an account, suspend account activity or file a suspicious activity report?

TEST: You should test your new program to ensure that it functions as intended. Ask the following questions:

- *Does internal audit or compliance review identify program shortcomings?*
 - Have we updated our internal audit procedures to incorporate reviews for compliance with USAPA requirements?
 - Does staff recordkeeping appear to provide an adequate compliance paper trail for our CIP and law enforcement response obligations?
 - Does an audit of sampled transactions identify CIP or other BSA/AML program deficiencies or regulatory violations?
 - Is our audit program sufficiently detailed to evaluate BSA/AML compliance including USAPA requirements? Is the frequency of audit reviews appropriate to our institution's money-laundering and terrorist financing risk profile? Does internal oversight have sufficient management independence and Board access to be effective?
 - Does the internal audit program or other reliable review sufficiently oversee the record of service providers upon whom we rely for complying with BSA/AML program or CIP obligations?
 - Have we responded to law enforcement information requests in as efficient and compliant a fashion as possible given our institution's resources?

- *Is staff and service provider implementation of regulatory requirements keeping pace with our operational needs?*
 - Are there performance gaps in the rollout of the program among staff that require an adjustment to, or rethinking of, resource allocation?
 - Are service providers faithfully executing their responsibilities under our new program and their own policies without a fall-off in operational productivity?
 - Do we need to shift responsibility for certain areas of compliance to other employees given the increased responsibility of our designated BSA officer?
 - Do we need to outsource some of our BSA compliance functions?
 - Does it appear that we need unanticipated enhanced technological capabilities in order to fulfill our program and regulatory obligations?
- *Is our updated BSA/AML program with CIP providing us with reliable assurances of regulatory compliance?*
 - Are there lessons learned from our initial experience or internal reviews that recommend improvements to our revised program?
 - What does customer reaction tell us about the operating success of our CIP or private banking procedures?
 - Is the staff conducting the program properly accountable to the Board? Are performance reports and audit reports reaching responsible senior officials?
 - Can we respond promptly to correct any deficiencies in our BSA/AML compliance program? Are corrective action recommendations tracked to assure completion?

The OTS believes that applying the ADaPT process will assist you in achieving timely compliance with the new USAPA requirements and establishing a comprehensive BSA/AML program.