

PATH

TO REVISIONS

BANK SECRECY & AMIL MANUAL



The Federal Financial Institutions Examination Council (“FFIEC”), the interagency body created to ensure uniform treatment and examination of financial institutions by the federal banking regulators, revised its Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual (“2006 Manual”). The revisions make significant changes to FFIEC guidance on risk assessment, the handling of ACH transactions, treatment of trade finance, suspicious activity reporting, politically exposed persons, private banking, due diligence, insurance products, stored value products, and other emerging money laundering risks. Some of the most important practical considerations include:

- For ACH transactions, both the originating and receiving institutions must have OFAC screens in place.
- In trade finance, institutions must adopt comprehensive consumer due diligence programs.
- Where the circumstances of a sale warrant, banks engaged in insurance agency activities may have to file SARs jointly with insurance providers.
- For stored value cards, institutions must adopt risk assessment and mitigation measures to address money laundering risk.

The 2006 Manual will be systematically relied upon by examiners as they carry out every bank examination in the United States, as well as laying the foundation for analysis by non-bank financial regulators for such sectors as broker/dealers, money services businesses, and insurance companies. Accordingly, all banks and most U.S. financial institutions will need to undertake a careful review of the 2006 Manual, and prepare to update their existing AML policies and procedures to take into account its new provisions.

Risk Assessment

The 2006 Manual contains a new separate section on risk assessment. The section expressly requires a comprehensive analysis of each institution’s BSA/AML risks by the AML officer in a process that includes and is understood by all relevant institution employers, officers and directors. Examiners are cautioned against requiring any particular format for a risk assessment.

The prescribed risk assessment consists of two main parts: identification of specific risk categories and a more detailed analysis and assessment of the risk posed by these particular categories. In evaluating an institution’s assessment of its risk categories, the examiner may find that the institution is involved in high-risk categories of products or services but that the institution’s BSA/AML program effectively mitigates those risks. Additionally, institutions are provided a certain level of flexibility in developing their BSA/AML risk assessments, as the Financial Crimes Enforcement Network (“FinCEN”) recognizes that the risk-factors are often bank specific. The guidance provides, by way of example, that a particularly high number of funds transfers may be viewed as higher risk, but not if those transfers are done primarily for long-term, well-known, domestic customers. Examiners are urged to consider not only the specific risks associated with specific products (e.g., stored value cards, money transfers, certain insurance products, trade finance activities) but also the manner in which the institution mitigates the potential risk (e.g., by enhanced due diligence programs, knowledge of customer and normal account usage, etc.). Part two of the risk assessment requires a more detailed analysis of the information relating to the risk categories to determine the extent to which the items in those categories actually pose a risk, given the institution’s BSA/AML program. The guidance notes that the analysis should consider the following factors, as appropriate:

- The purpose of the account;
- The actual or anticipated activity in the account
- The nature of the customer’s business;
- The customer’s location; and
- The types of products and services used by the customer.

Automated Clearing House (ACH) Transactions

The new regulatory focus on the use of ACH transactions to launder money is reflected in a new section in the 2006 Manual, which specifies the risks associated with ACH transactions and provides guidance to financial institutions on how to mitigate those risks. The specified ACH risks include transactions involving the original payment (or subsequent payments) into accounts opened via the Internet, where there is no face-to-face contact; transactions originated through third-party service providers; and situations where neither the third-party service provider nor the originating financial institution performs the required due diligence on the entities for whom they are originating payments. The 2006 Manual also specifies certain types of ACH transactions that may be more prone to fraud or manipulation, including: originating financial institutions authorizing a third-party service provider to send ACH files to an ACH operator such that the originating financial institution is bypassed; originating and receiving financial institutions relying on each other to perform the required due diligence on customers; and processing of ACH transactions being highly automated with minimal opportunity for human review and/or analysis.

The 2006 Manual recommends risk mitigation through:

- Obtain sufficient customer due diligence (“CDD”) information.
- Develop and implement an effective risk-based suspicious activity monitoring system that takes into consideration the characteristics and risks of ACH transactions.
- Review the suspicious activity monitoring policies and procedures of third-party service providers.
- Consider the layering and integration states of money laundering when assessing the risk of a particular ACH customer.
- Consider developing and implementing a separate process for reviewing international ACH transactions.

The 2006 Manual also discusses the Office of Foreign Assets Control (“OFAC”) requirements on originating and receiving financial institutions involved in ACH transactions. For the first time it specifies that both ends of a transaction must be subject to OFAC screening: the originating financial institution is responsible for making sure that the originator is not a blocked party; the receiving financial institution is similarly responsible with respect to the receiver. While this has previously been OFAC’s position, this is the first time the requirement has been expressly mandated within the examination process.

Trade Finance Activities

The 2006 Manual finds that trade finance activities, which typically involve short-term financing to facilitate the import and export of goods, can present a risk because of the number of individuals, and financial institutions, involved. Additionally, the document-intensive nature of trade finance relative to other banking activities also increases the potential risk. Accordingly, FFIEC recommends that financial institutions undertake comprehensive CDD programs for trade finance that enable an institution to be knowledgeable both about the persons involved and the jurisdictions involved in the transaction.

The 2006 Manual provides extensive guidance on the types of CDD that institutions should consider, including the use of background checks on individuals and the reviewing of paperwork and other documentation for potential red flags. Such red flags may include over- or under-charging for the value of the shipment, discrepancies in the description of the items being shipped, or other anomalies. The guidance notes that even though one of these anomalies may be present, it may not be necessary to file a suspicious activity report (“SAR”), but rather the institution should perform further investigation. Even when a SAR is required, the institution is not necessarily required to stop the transaction (although a transaction involving an OFAC violation must be stopped, of course).

Regulatory and Supervisory Guidance

The 2006 Manual makes several key additions to the guidance provided on suspicious activity reporting, specifically related to the SAR decision-making process, the timing of a SAR filing, and the sharing of SARs with head offices and controlling companies.

The 2006 Manual continues to recognize that the decision to file a SAR is a subjective one, and continues to encourage banks to document SAR decisions. The new guidance, however, elaborates on the documentation issue. The guidance notes that there is a wide variety of systems used by different institutions to monitor, track, and identify transactions, and that each SAR decision will likely involve a unique set of facts, there is no single form that should be required when a bank decides not to file a SAR. Thus, institutions maintain a certain level of flexibility in how they document their respective SAR filing decisions.

There is also additional guidance regarding the timing of a SAR filing. Specifically, the guidance elaborates on the phrase “initial detection” and clarifies that the phrase should not be interpreted to mean the very moment that a transaction is highlighted or flagged for review. Recognizing that many completely normal transactions, such as a major purchase, an inheritance, or a gift, may be viewed by the BSA/AML system as being unusual or inconsistent with respect to a given account or customer, even though the transacting is completely legitimate. The flagging of such a transaction by the institution’s automated system should not be viewed as the “initial detection” of the transaction. Interagency guidance issued in January 2006 regarding the sharing of SARs with head offices and controlling companies is incorporated into the 2006 Manual. The guidance provides that controlling company includes:

- A bank holding company (“BHC”), as defined in section 2 of the BHC Act;
- A savings and loan holding company, as defined in section 10(a) of the Home Owners’ Loan Act; or
- A company having the power, directly or indirectly, to direct the management policies of an industrial loan company or a parent company or to vote 25 percent or more of any class of voting shares of a industrial loan company or parent company.

The incorporated guidance also confirms that a U.S. branch or agency of a foreign bank may disclose a SAR to its head office outside of the United States, and that a U.S. bank may disclose a SAR to controlling companies regardless of whether they are domestic or foreign. It is important to note that the guidance does not permit banks to share SARs with affiliates other than a controlling company or head office, although the information underlying the SAR filing may be disclosed to affiliates.

Foreign Correspondent Account Recordkeeping and Due Diligence

In January 2006, FinCEN published a final regulation implementing due diligence requirements relating to foreign correspondent accounts. The 2006 Manual provides guidance in accordance with this new regulation, providing that due diligence policies, procedures, and controls must include:

- Determining whether each such foreign correspondent account is subject to enhanced due diligence;
- Assessing the money laundering risks presented by each such foreign correspondent account; and
- Applying risk-based procedures and controls to each such foreign correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose, and anticipated activity of the account.

In addition to the above requirements, the guidance notes that the regulation requires an institution’s due diligence program to include special procedures when appropriate due diligence cannot be performed with regard to a foreign correspondent account. Under 31 CFR

103.176(a), the due diligence program must include criteria for when the bank should refuse to open the account, suspect transaction activity, file a SAR, or close the account.

Also in January 2006, FinCEN issued a Notice of Proposed Rulemaking that would implement enhanced due diligence requirements relating to certain foreign banks. As this regulation is not yet finalized, the 2006 Manual reiterates the guidance provided in the prior version of the BSA/AML Manual that institutions incorporate due diligence policies and procedures based on the statutory requirements of 31 USC 5318(i)(2).

Private Banking Due Diligence

The 2006 Manual provides new guidance relating to mitigating the risk of shell companies, including “maintaining control of bearer shares, entrusting the shares with a reliable independent third party, or requiring periodic certification of ownership.” The guidance allows, however, that an institution may distinguish its controls between new clients and long-term, well-known clients.

Insurance

Last November, FinCEN issued two final rules imposing AML requirements on insurance companies.⁸ The final rules cover only those insurance companies that sell products identified by FinCEN as being highly vulnerable to potential money laundering or terrorist financing activities. Specifically included are permanent life insurance policies, annuity contracts, and “[a]ny other insurance product with features of cash value or investment.”⁹ The rule excludes insurance agents and brokers from the definition of “insurance company,” based on recognition that insurance companies bear the risk of the various products and that they are also better situated to absorb the cost of implementing an AML program.

The 2006 Manual provides that if a bank, acting as an agent of the insurance company, detects unusual or suspicious activity, it is permissible to file a joint SAR with the insurance company. The guidance also expanded on prior examples of suspicious insurance transactions to include purchasing insurance products through unusual methods such as currency or currency equivalents, or buying products with insurance termination features without concern for the product’s investment performance.

Politically Exposed Persons

Recognizing that it may be difficult to ascertain if a given individual qualifies as a “politically exposed person” (“PEP”), the guidance provides that institutions should take all reasonable steps to avoid unknowingly or unwittingly hiding or moving any proceeds of corruption by senior foreign political figures or associates. As with other BSA/AML requirements, the institution’s controls and procedures should be risk-based.

Noting that a title alone cannot be relied upon to determine that an individual is or is not a PEP, the 2006 Manual identifies several factors that an institution should consider when making such a determination, including: the official responsibilities of the individual’s office; the nature of the title (honorary or salaried); the level of authority over government activities or other officials; and access to significant government assets or funds. In determining whether a person is a “close associate” of a PEP, institutions are advised to focus primarily on relationships that are “widely and publicly known.” Although this is a somewhat limiting factor, the guidance also provides that where an institution has actual knowledge of a close relationship, even if it is not widely and publicly known, the institution is required to consider the person a PEP.

In keeping with the requirement that BSA/AML programs be risk-based, the guidance recognizes that not all PEPs present an identical level of risk. Factors to be considered in evaluating the level of risk posed by a particular PEP include: where the individual is, his or her position or authority, the size or complexity of the account relationship, and the products or services involved in the account relationship.

Emerging Money Laundering Risks – Stored value Cards

The U.S. Money Laundering Threat Assessment (“Threat Assessment”), issued in December 2005, evaluated the potential money laundering risk of stored value cards and other electronic cash instruments. The 2006 Manual incorporates some of the information covered by the Threat Assessment, noting the various methods by which criminals have utilized stored value cards to move illicit funds without detection. The guidance warns institutions that because stored value cards are easy to fund, easy to transport, and create no paper trail, they are often attractive to criminals – for example, drug dealers who send loaded, prepaid cards to drug suppliers effectively send “cash” with little to no risk of detection. Thus, the 2006 Manual provides the first direction to examiners to include within their examination process a review of whether the financial institution has undertaken an adequate risk assessment and mitigation measures to address money laundering risk associated with stored value cards.