

# **The 2006 FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual:**

## **Knowing the Risks – Is It Possible to Keep Pace and Manage Them All?**

**By: Carmina Hughes, Executive Director and  
Patricia McKeown, Managing Director  
Daylight Forensic & Advisory, LLC**

### **I. Background**

On July 28, 2006, the Federal Financial Institutions Examination Council (“FFIEC”), comprised of the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision released the revised Bank Secrecy Act/Anti-Money Laundering (“BSA/AML”) Examination Manual, updating and retiring the June 2005 Manual.

In its continuing efforts to provide guidance to financial institutions to facilitate compliance with the Bank Secrecy Act, the FFIEC has endeavored to incorporate additional information, regulatory updates, and feedback from both the financial services industry as well as its examiners.

There are some significant changes to the revised Manual, and the regulatory expectations are clear - financial institutions must be able to identify and manage the potential risks of money laundering, terrorist financing and evasion of sanctions of the Office of Foreign Assets Control (“OFAC”). But are financial institutions truly able to manage these potential risks, and are the expectations realistic? Are the tools and technology available, and how can institutions keep pace in an environment of new and evolving risks?

### **II. What has Changed?**

The FFIEC has incorporated regulatory updates effective since the release of the June 2005 manual. These areas include additional information and guidance on Politically Exposed Persons (“PEPs”), Suspicious Activity Reports (“SARs”), Insurance, Foreign Correspondent Account Recordkeeping and Due Diligence, and Private Banking Due Diligence. These are all critical areas, some of which – particularly the new requirements of the Final Regulation for Section 312 - financial institutions continue to struggle with both in implementation and compliance.

This article will address the FFIEC’s increased focus on the risk assessment as well as new information on potential areas of risk – ACH, trade finance, stored value cards and nominee incorporation services. The FFIEC has provided new

information that serves to outline the regulatory expectations. It's now up to the financial institutions to manage the risks accordingly - but have the tools and technology kept pace with regulatory expectations, and are the expectations realistic?

### **III. Assessing and Managing the Risks – but They Keep Changing!**

#### **A. In the Beginning - The Risk Assessment**

There should be no doubt as to the importance of financial institutions conducting and utilizing a risk assessment to identify, monitor, manage and mitigate their risks. Although guidance on the BSA/AML risk assessment was included in the June 2005 Manual, the new Manual places much greater emphasis on the regulatory expectation for the risk assessment process. The risk assessment should be the foundation of a BSA/AML and OFAC compliance program, and the program - training, monitoring, independent testing, etc. should evidence sufficient controls to manage the identified risks. In addition, organizations adopting an Enterprise-Wide Approach to their BSA/AML risk assessment must assess the risks presented in all subsidiaries and legal entities. This approach anticipates Enterprise Wide Compliance and Risk Management and incorporates assessing risks across the entire organization as well as down through the business lines.

In summary, the risk assessment should be the starting point for a comprehensive AML program. The risk assessment is a living document, subject to continual change as the organization changes with the identification and addition of new and changing risks.

<p>The Risk Assessment: 5 Tips for Success</p> <ol style="list-style-type: none"><li>(1) The BSA/AML/OFAC risk assessment should incorporate the risks of money laundering and terrorist financing across the institution including an evaluation of all legal entities as well as all business lines;</li><li>(2) Leadership and involvement from the top of the organization is critical;</li><li>(3) Build from the foundation up, making the risk assessment the starting point of the BSA/AML/OFAC program;</li><li>(4) Include products and services, customer types, geographies, and anticipated activity; and</li><li>(5) Have ongoing communication and training to ensure an understanding of the process as well as the importance of protecting the organization and complying with the law.</li></ol>
---

#### **B. Evolving Risks - Traditional Services with Changing Risk Profiles**

Although completing the risk assessment is a great accomplishment, the stiffest challenges lie ahead. A risk profile is never static. While an institution is ensuring that its compliance program is risk-based and reflective of the risks identified – the risks are often changing at the same time that the program is being defined and implemented.

The 2006 FFIEC manual has added guidance on Automated Clearing House (“ACH”) Transactions and Trade Finance Activities. Both of these are traditional services offered by financial institutions, but the potential risks for money laundering, terrorist financing, and even the attempted evasion of OFAC sanctions, have increased as these services are more widely used. Following is a brief discussion of both of these services – and how the risks have changed.

#### ACH:

The ACH network has been in place for 35 years. ACH has historically been utilized primarily for recurring domestic payments, particularly for payroll or payments such as mortgages, thus presenting a very low risk of money laundering.

However, the volume and amount of ACH transactions have increased dramatically. Additionally, the once largely domestic payments system has taken on an international flavor. Cross-border payment services are currently available to Canada, Mexico, Austria, Germany, the Netherlands, Switzerland and the United Kingdom – and services are expected to expand to other geographies. The origination of ACH transactions is also changing with increasing use of electronic banking, the internet and the phone.

The popularity and growth of the ACH network presents new and growing challenges to financial institutions – and current systems, processes and procedures may not have kept pace with the evolving risks.

For example, ACH is no longer being used solely for the transactions for which it was designed - low-dollar routine credit and debit transactions originated and received by customers of financial institutions. ACH transactions may be originated by third parties (i.e. entities other than the originator, Originating Depository Financial Institution or the Receiving Depository Financial Institution that perform any functions on behalf of these entities for ACH processing), and risks are heightened if the third party has not conducted due diligence on the companies on whose behalf it is originating payments. In some cases, Originating Depository Institutions and Receiving Depository Institutions may rely on each other to conduct reviews and screenings for due diligence as well as OFAC compliance. The institution may not know the third party, the purpose of the transaction or the source of

funds. In addition, if the transaction file is sent in a batched format and is not opened, the ACH transactions being processed may not be susceptible to review for suspicious activity during processing. At this point, a financial institution may have in place a transaction monitoring system, procedures and processes for detecting suspicious activity – but due to the constantly changing environment, suspicious activity may not be detected with current processes and capabilities.

Though ACH transactions in the past may have been considered a low risk for money laundering and OFAC violations, these risks are on the rise. The growth in the number and size transactions and the ease of originating transactions through various channels and geographies available have all added new risks to manage. So what should financial institutions do to protect themselves and the financial system from these new risks?

**Tips for Protecting Your Institution’s ACH Transaction Processing:**

- (1) Ensure that effective Customer Due Diligence (“CDD”) policies, procedures, processes and controls are in place and being followed.
- (2) If using a Third-Party Service Provider (“TPSP”), the financial institution utilizing its services should conduct due diligence to know the Provider and understand its due diligence programs for companies for whom they are originating payments.
- (3) Due diligence policies and procedures should include processes and procedures for restricting or refusing ACH transactions if suspicious and/or potentially illegal activity is suspected.
- (4) Ensure that ACH transactions are screened by a robust transaction monitoring system – and that due diligence conducted on any third parties includes a review of their monitoring systems as well.
- (5) Ensure heightened awareness, screening and procedures for international transactions.

**Trade Finance:**

Trade finance is another standard line of business for financial institutions, but as with ACH, trade finance can involve multiple parties, multiple geographies – and the money laundering, terrorist financing and OFAC risks surrounding these activities has grown.

Financial institutions are involved in trade finance activities at many different levels, presenting many challenges to the institution to truly know the parties involved the type of goods and industry, as well as different geographies. Trade finance, which typically involves short-term financing to facilitate the import and export of goods, includes services such as letters of credit, standby letters of credit and guarantees. They often involve multiple parties and multiple financial

institutions, creating uncertainty in knowing the customer(s) and parties, as well as understanding of the transaction.

Additional risks are posed from a documentary standpoint if the financial institution is not familiar with the type of goods involved and their pricing. Because trade finance relies heavily on documentation presented, the risk of fraudulent documentation is high, and banks must implement policies and procedures to mitigate these risks. In addition, although financial institutions cannot be expert in all types of goods being imported or exported, the financial institution should be aware of the value of goods - particularly high priced and high risk goods as well as attempts to over- or under-value the goods in order to evade regulations.

**Tips for Managing the Risks of Trade Finance Activities**

- (1) Ensure that your institution has in place effective BSA/AML/OFAC policies, procedures, processes and controls with regard to trade finance;
- (2) Ensure that processes and procedures include a review process to identify possible fraudulent documentation;
- (3) Be aware of the red flags – such as transactions to or from high risk geographies or transactions of goods determined to be high risk that appear to be over- or under-valued;
- (4) Ensure that all transactions are effectively monitored for suspicious activity; and
- (5) Ensure that all transactions and parties to the transactions are screened for OFAC compliance.

**C. New Threats: New Products and Services**

In December 2005, the Treasury Department and its partner agencies released the 2005 Money Laundering Threat Assessment (“MLTA”), the first government-wide analysis of money laundering in the United States. This document details various money laundering methods - some well-known and others new and innovative.

The FFIEC Manual incorporates some of the threats identified in the Money Laundering Threat Assessment. In particular, the revised manual incorporates two threats that will be discussed here – stored value cards and nominee incorporation services.

**1. Stored Value Cards**

Stored value cards are increasing in popularity due to their ease of use – both for legitimate purposes as well as illegal purposes such as money

laundering and terrorist financing. Open system stored value cards may be utilized in global ATM networks for purchases or ATM withdrawals worldwide. A bank account is not required, and the cards can be purchased by one individual and passed along to another. The cards can typically be reloaded – offering the ability to add value and reuse the card indefinitely. Closed system cards do not offer as much opportunity and flexibility as the open system cards, as these cards are often limited to specific merchants or services, and typically cannot be reloaded.

Stored value cards may be purchased at various financial institutions – but they can also be purchased worldwide, through various channels such as the internet, and often the cards do not have cash limits. Depending on the country and selling entity, purchaser’s identification may not be captured thus allowing for anonymous exchanges of currency. The impediment to enforcement and investigation is clear.

To make the cards even more vulnerable to illicit use, many stored value card programs are processed by a third party utilizing a “pooled” bank account in the name of the third party managing the program. In this case, individual card transactions may not be identifiable for monitoring suspicious activity.

Although not strictly required by the Customer Identification Program (“CIP”) regulation, guidance provided in the FFIEC manual encourages financial institutions to capture information on the purchaser of stored value cards. However, there are limitations in how this information can assist in the identification of suspicious activity or the illegal use of the cards. If the cards are sold to customers, the financial institution may have sufficient customer due diligence information on file. However, if the cards are sold to non-customers, the institution will not know the source of funds or the anticipated use of the card – or who will ultimately use the card. In addition, the financial institution may be utilized for providing payments from the stored value cards in the form of cash withdrawals from its ATM network. The financial institution may not be able to identify the individual using the card – and would not be able to trace the source of funds for the transaction.

- |   |
|---|
| <p>Tips for Protecting Your Institution – Stored Value Cards</p> <ol style="list-style-type: none"><li>(1) Effective CIP policies, procedures and processes should be developed and implemented to address the sale of stored value cards;</li><li>(2) Financial institutions should consider setting card limits and implementing other controls; and</li><li>(3) Financial institutions should ensure that stored value card transactions are monitored for suspicious activity. This may include transaction monitoring systems, the review of manual reports, or other tools.</li></ol> |
|---|

2. Nominee Incorporation Services (“NIS”)

Another area of risk incorporated into the July 2006 FFIEC manual from the 2005 Money Laundering Threat Assessment originates from NIS. Nominee incorporation services establish U.S. or foreign shell companies and bank accounts on behalf of foreign clients. NIS, established as intermediaries, can serve legitimate purposes in the cases where the company is properly licensed, the purpose is legitimate and the beneficial owners seek anonymity.

However, NIS are often employed to further illicit purposes such as money laundering and terrorist financing. Companies established by NIS are typically formed in jurisdictions that enable them to obfuscate the identity of the beneficial owners and purpose of the company, hide the source of assets involved, and require little recordkeeping and documentation. NIS may form companies in the United States or offshore. The new company may be incorporated in an Offshore Financial Center offering anonymity and tax benefits, the company may be established with bearer shares adding to the difficulty in determining ownership. Bank accounts may then be established through the internet and funds transfers may be sent worldwide, possibly to high risk jurisdictions.

So how can banks overcome these risks?

Tips for Identifying and Monitoring Nominee Incorporation Services

- (1) Ensure that CIP policies, procedures and processes are effective in gathering sufficient information to not only identify Nominee Incorporation Services – but also to identify the beneficial owners, purpose, source of funds/assets, anticipated activity and other relevant information.
- (2) Ensure staff are able to identify a shell company:
  - a. Entity may not have a physical presence other than a mailing address;
  - b. Entity may be public traded or privately held;
  - c. Entity has no employees and produces nothing;
  - d. There may be difficulty in determining the beneficial owners, and the use of bearer shares may add further difficulty in identifying the owner(s);
  - e. In the United States, shell companies are often formed in Delaware, Wyoming and Nevada.
- (3) Ensure that account opening and other staff throughout all business lines are aware of the red flags for suspicious activity, and that policies and procedures include steps to be taken if suspicious activity is

suspected – including the refusal to open or the closing of an existing account.

(4) Ensure that systems and/or processes are in place to monitor these accounts.

### **III. How to Keep Pace?**

Although guidance is provided on how financial institutions should identify, monitor and manage their money laundering, terrorist financing and OFAC risks – the risks are constantly changing. It takes time, effort and resources for institutions to move through the risk identification and assessment process: policies, procedures and controls are established; processes and systems for the monitoring and identification of suspicious activity are implemented; staff are trained; and independent testing is planned to be risk-based in execution. However, while these efforts are ongoing – the risks continue to change and new threats emerge. Traditional products and services may now be used in ways such that they pose new risks, and new product and service offerings pose new risks altogether.

How can financial institutions keep pace?

In order for financial institutions to be in compliance with BSA/AML and OFAC laws, regulations and regulatory expectations, the institution must have the resources, knowledge and commitment to implement and sustain a successful program. Will risks keep changing? Absolutely. However, efforts must be ongoing. Financial institutions must be continually vigilant, as the risks of money laundering, terrorist financing and potential OFAC violations may be changing faster than the technology and tools in place.

The reality is that financial institutions may not be able to keep pace with the constantly changing threats, but there are steps that can be taken to ensure a reasonable and effective approach:

- (1) **Tone at the Top.** The Board of Directors and Senior Management should set the tone of the organization. The importance of their involvement in the institution's BSA/AML/OFAC compliance program cannot be overstated. They should receive regular communication and updates, and in turn they should communicate information and expectations throughout the organization.
- (2) **The Risk Assessment – an Ongoing Reality.** The risk assessment is not a static document, but a process that requires continuous updating. The initial process may be time consuming and resource-intensive. But continuous updating is necessary to enable the organization to keep pace with new and changing risks.

- (3) Resources. In order to keep pace with the changing landscape, sufficient resources must be dedicated to BSA/AML/OFAC compliance, and these individuals must keep abreast of ongoing changes. Additional resources are not only an impact to the organization's bottom line – the resources may also be hard to find and a challenge to retain.
- (4) Tools and technology. Although tools and technology may be in place to monitor existing risks to the institution – the tools and technology must also be continually reassessed. New tools and technology may need to be implemented, or thresholds of existing systems and processes may need to be changed.
- (5) Training. Training of employees must be ongoing, comprehensive and continually updated. Employees should have an understanding of the importance of compliance – but also the awareness of the potential consequences of non-compliance to themselves, the organization and its shareholders.

#### **IV. Conclusion**

The risks of money laundering, terrorist financing and OFAC violations to financial institutions are changing, and they will continue to change. These risks may occur in traditional product lines or entire lines of business. New products and services, new lines of business, the expansion of geographical capabilities, delivery channels and other changes will bring all new risks. Financial institutions must be able to react accordingly – but it will only be with the continual assessment and re-assessment of and commitment to their BSA/AML/OFAC programs that institutions will successfully manage the risks in an ever-changing landscape.