

How to Implement Risk-Based OFAC Monitoring Practices

BY TIMOTHY R. WHITE, CAMS

The banking industry has entered a new era in Office of Foreign Assets Control (OFAC) compliance, recognizing that there is no one right way to monitor for OFAC compliance when implementing a risk-based approach.

This article provides five steps to structuring risk assessment, and examines 10 risk-based OFAC monitoring practices. Most of these practices are used by large money center banks that have long been accustomed to the risk-based balancing act of staying in obedience with OFAC and their federal examiners. Community and regional banks can achieve significant efficiencies by emulating larger institution's practices in light of the new risk-based exam procedures.

OFAC and the Financial Institutions Examination Council (FFIEC) are to be commended for their foresight in identifying that a risk-based OFAC compliance regime dovetailed with a risk-based Bank Secrecy Act (BSA)/anti-money laundering (AML) program provides the most efficient allocation of OFAC compliance resources. In the 2005 *BSA/AML Examination Manual* (updated in 2006),¹ the scope and procedures for OFAC compliance are vastly expanded, and risk-based compliance and transaction monitoring were both introduced. These two concepts were completely absent from the previous OFAC exam procedures introduced in 1996.²

Overall, the banking industry has done a remarkable job of abiding by the many sanctions programs administered by OFAC in the interest of enforcing U.S. foreign policy. The relatively small number of civil monetary penalties that OFAC has levied further demonstrates the industry's solid compliance record. However, many low-risk community and regional banks are challenged by the adoption of the 2005 standards. A large number of smaller institutions and a few regulators alike are struggling to apply the methodology of an enterprise-wide risk-based OFAC program to low-risk environments.

Risk Assessment: The Cornerstone of an Efficient OFAC Program

Many banks have been slow to adopt a risk-based approach because their institutions are low risk, they already use interdiction software, or they have never had any

OFAC issues and it is very unlikely they ever will. Nonetheless, these institutions have an obligation to assess their risk. Three vital elements for a successful OFAC regulatory exam is for a bank to understand its risk factors, implement monitoring procedures commensurate with its risk profile, and effectively communicate this to its examiner. By accurately assessing, identifying, and documenting the bank's overall OFAC risk, the bank can efficiently allocate resources for monitoring. A comprehensive risk assessment will also communicate to your examiner that you understand what a risk-based approach entails. Otherwise, a low-risk bank may appear to the examiner as an inexperienced bank. Without the regulator's confidence in the bank's OFAC risk assessment, the bank will likely be subject to more intense scrutiny and criticism, and the OFAC portion of the BSA exam will be off to a problematic start.

Five Steps to Structure OFAC Risk Assessment

1. Know What is on the OFAC List

When conducting a thorough OFAC risk assessment, consider the likelihood of your institution's encountering a real OFAC hit or match.³ To do this, it is necessary to understand what is on the OFAC lists.

Of the thousands of records on the various OFAC sanction lists, about 62 percent are Hispanic surnames, due to the fact that Specially Designated Narcotics Traffickers (SDNT) is OFAC's largest sanctioned category. Most of the SDNTs and Specially Designated Narcotics Trafficking Kingpins (SDNTKs) are from Central and South American Spanish-speaking countries. In addition to narcotics traffickers, the database contains the embargoed country of Cuba and members of several South and Central American terrorist organizations. Fewer in number but of the highest national concern are Specially Designated Global Terrorists (SDGTs), Specially Designated Terrorists (SDTs), Foreign Terrorist Organizations (FTOs), the Non-Specially Designated Pales-



Five Steps to Risk Assessment 10 Practices for Monitoring

tinian Legislative Council (NS-PLC), and the Non-Proliferation of Weapons of Mass Destruction (NPWMD) lists. Combined, these groups account for roughly 21 percent of OFAC's identified entities. The remaining 17 percent are affiliated predominately with U.S. sanctions and embargoes (Balkans, Belarus, Burma, Democratic Republic of the Congo, Iran, Iraq, Liberian Regime of Charles Taylor, North Korea, Sudan, Syria, and Zimbabwe). These numbers are as of the June 15, 2007, OFAC update; keep in mind that the number of Specially Designated Nationals (SDNs), aliases, and sanction programs is continually growing.

Armed with knowledge of what is on the list, a bank can carry out and document an OFAC risk assessment. A logical first step is to expand the bank's organization chart to include an assessment of each department's risk factors:

2. Identify Each Departments OFAC Risk Factors

According to the FFIEC, an effective risk assessment "should be a composite of multiple factors, and depending on the circumstances, certain factors may be weighted more heavily than others."⁴ Factors to identify include the following:

Customer Types⁵

- nonprofit and charitable organizations
- international customers (commercial and retail)
- students
- non-resident aliens (NRAs)

Products and Services

- letters of credit
- foreign exchanges
- Society for Worldwide Interbank Financial Telecommunications (SWIFT) messages
- wire transfers
- cash purchases (large denominations)

Types of Transactions

- large amounts
- high frequency

Account and Transactions Parties

- originators, intermediaries, beneficiaries
- principals, guarantors, beneficial owners, nominee shareholders, directors, signatories, and power of attorney

Locations or Involved Geographies

(See map on page 12)

- international items
- proximity to Canadian and Mexican borders
- proximity to major cities
- high intensity financial crime areas (HIFCA)
- high intensity drug trafficking areas (HIDTA)

3. Evaluate and Rate Each Risk

Once the risk factors within each department are identified, evaluate how these risk factors match up with the examination manual's Appendix M: Quantity of Risk Matrix OFAC Procedures.⁶

4. Document

Document the OFAC risk assessment for each and every OFAC exposure using an OFAC risk decision template (see sidebar). Copies of each completed decision template should be maintained as part of the written OFAC monitoring program.

OFAC Risk Decision Template

OFAC issue: Screening payees on on-us checks within the normal automated process

Decision made: Not to screen payees on on-us checks within the normal automated process.

Date: September 19, 1999

Who was involved in the decision-making process: Mary Miller and Sam Smith

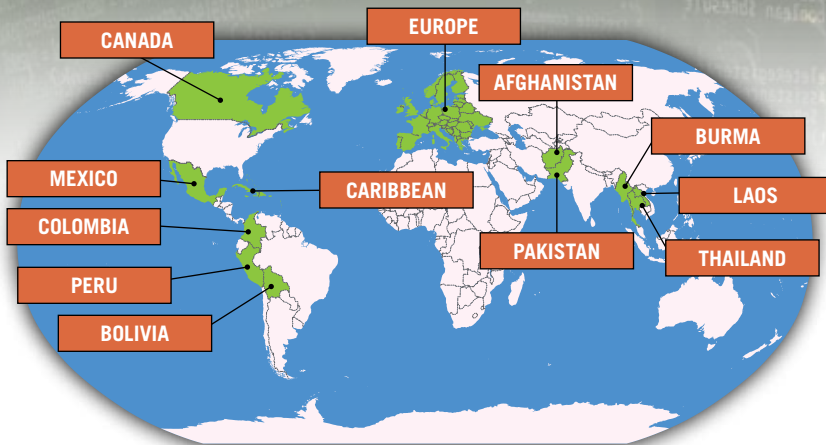
Associated risk: Low

Justification of decision: Screening payees on on-us checks is not an effective use of compliance resources (time and money) because the information is not in an electronic format that is conducive to automating the screening process and the volume of items is prohibitive.

COURTESY OF HANK GRANT & ASSOCIATES⁷

5. Summarize

The summary should include an enterprise-wide risk assessment as well as specifically listing high-risk OFAC locations, departments, transactions, and customers. Include details for monitoring each calculated risk. Establish procedures to communicate this to department personnel and examiners. These findings will enable the bank to "... establish and maintain an effective, written OFAC program commensurate with their OFAC risk profile ..."⁸ as defined in the *BSA/AML Examination Manual*, 2006. Keep in mind, these findings will also serve as the foundation for the bank's designated OFAC officer to structure written policies, pro-



Drug Transshipment Countries and Regions⁹

cedures, and processes; provide on-going training and they will assist with the required independent testing, as outlined in the BSA/AML Examination manual, 2006.

10 Risk-based OFAC Monitoring and Screening Practices

The following baselines and best practices are skewed toward aiding community and regional banks as opposed to the money center banks. These screening standards should be viewed in general terms and not as legal advice, because a combination of unique factors could place an OFAC sanctions monitoring obligation on virtually any element of your institution's operation.

1. Screen All International Accounts and Transactions

Because of the international nature of sanction programs it is imperative that financial institutions pay close attention to all accounts and transactions that involve international entities and destinations. Federal examiners are keenly focused on a financial institution's ability to monitor for international entities. Unless your institution's OFAC risk assessment has appropriately eliminated the OFAC risk associated with a particular international item, this item should be screened. Regulators are likely to view all international items as high risk. Choosing to disregard OFAC screening on any international item may raise a red flag with regulators and cause them to question the accuracy of the bank's risk assessment. OFAC compliance wisdom would suggest erring on the side of caution and conservatism when dealing with transnational items.

2. Screen All Wire Transfers

Wire transfers are the highest risk transactions for many institutions and should be screened in real time prior to execution. Wires usually involve large dollar amounts and are immediate and nonretrievable. The electronic formatting of wire transaction information is easily screened by the receiving or intermediate financial institution's interdiction software. Consequently, if a wire involves a sanctioned entity and you did not catch it prior to execution, the receiving institution will most likely report your violation to OFAC.

3. Monitoring of Real-Time, Face-to-Face Transactions at the Teller Lines

Many institutions and a few regulators alike waste valuable resources by being over-prescriptive with their OFAC monitoring standards in this area. A commonsense, risk-based approach can greatly benefit community and regional institutions. Money center banks have long employed sound risk-based monitoring in this environment. Seldom do they screen payees on low-dollar on-us checks and monetary instrument sales. They have rated these transactions as low risk, particularly at dollar amounts below the threshold of requiring a supervisor's approval. Front-line tellers should be charged to use their own instincts and refer any transaction to a supervisor for an OFAC approval. When the transaction rises to the supervisory level, the OFAC screening decision is made by the supervisor, who is the second tier of front-line OFAC risk assessment. This two-tiered risk-based OFAC procedure enables efficient and effective OFAC controls without being so prescriptive as to require tellers to screen all payees on every item. A commonsense approach in this area will almost always support the low-risk designation. SDNTs and SDGTs are not likely to be cashing low-dollar checks; bad guys tend to deal in cash because it is anonymous.

4. Screen All New Accounts

The FFIEC manual says that new accounts should be reviewed against OFAC lists "prior to being opened or shortly thereafter (e.g., during nightly processing)."¹⁰ This is another area where monitoring procedures are often too prescriptive. Many small, low-risk financial institutions conduct OFAC checks in real time amidst the other obligations of the account opening process. If this type of OFAC procedure poses no challenge there is no need to change it. However, many institutions have elected to screen their new accounts in a batch process at the end of the day. A centralized back office screening environment provides a safer and more efficient OFAC procedure than does a real time review. Below are six benefits to applying a back-office approach to new account screening:

- Reducing the exposure from a violent reaction: If a prospective customer has a substantially similar name to an SDN, that person has probably faced OFAC issues in the past. The bank has a PR exposure if the customer loses composure in the bank's lobby.
- Minimizing the disruption of workflow: Nightly batch screening will save time in the account opening process and

eliminate front-line time lost reviewing potential hits.

- Allowing a higher standard of review if done by an OFAC specialist.
- Simplifying and minimizing software fees and implementation issues: Interdiction software for real-time screening of new accounts often requires substantial fees for multiple seat licenses or multiple Internet login capabilities.
- Simplifying and minimizing training issues.
- Avoiding the problem of potentially rejecting an account opening that should be opened and blocked.

5. Screen All Existing Accounts Regularly

The bank's policies and procedures should address how the bank will identify and review existing accounts for possible OFAC violations. This is one of the few areas where OFAC compliance has changed very little with a risk-based approach. Since 1996, examiners have asked compliance officers "Are established accounts regularly compared to current OFAC listings?"¹¹ The new exam manual implies that low-risk banks can manually filter for existing accounts. The key consideration that has been added to this area of OFAC exposure is the concept of available technology. A financial institution that performs its own core processing or maintains a customer information file data warehouse can license excellent OFAC interdiction software, including an enhanced data update service, for a reasonable fee. A bank that has outsourced its core processing to a service bureau and does not maintain a CIF data warehouse may have to rely on the OFAC technology being provided by the service bureau. These third-party processing environments can limit how often they will screen your accounts. The manual states that banks should check existing customers when there are additions or changes to the OFAC lists, offering the following example: "banks with a low OFAC risk level may periodically (e.g., monthly or quarterly) compare the customer base against the OFAC lists."¹² However, the best practice for OFAC concerning existing accounts is to screen against every OFAC update within a 24-hour time frame. If a bank's customer gets placed on an OFAC list, that customer is likely to know right away and will pull his or her money from his or her account without delay.

6. Domestic ACH Transactions

At first glance, OFAC monitoring of domestic Automated Clearing House (ACH) seems an impossible task. However, if you replicate the risk-based approach used by large money center banks, the task turns into a very manageable know your customer (KYC) exercise. With few exceptions, large ACH originators are not filtering live domestic ACH transactions files. Their ACH OFAC compliance methodology shifts the monitoring from the real-time transaction file environment to a program designed to know your ACH originator. This customer due diligence approach is both sound and

cost-effective as it eliminates the following problematic elements of trying to filter live ACH transaction files:

- ACH transactions often contain insufficient information to permit adequate scrutiny of transactions for OFAC compliance. Many domestic ACH transactions contain minimal information (amounts, customer numbers, and account numbers), yet an effective transaction screening program requires detailed information such as full names and addresses. This detailed information enables compliance professionals to distinguish real hits from false positives. Without detailed data every hit becomes inconclusive.
- ACH transaction files have specific formats in that all items in the batch are totaled at the end as a payment instruction. For example, an ACH file consists of 1,000 transactions totaling \$222,123.45. How should a bank process the 10 to 20 hits that are in this file? Should it hold up the entire file or strip off the transactions that contain the hits and reformat the file for further processing? The ACH industry would come to halt if banks held up entire files. Reconciling and reformatting these files also present complex challenges.

To further bolster a customer due diligence approach to ACH OFAC compliance, it is imperative for the Originating Depository Financial Institution (ODFI) to develop a systematic approach for regularly disseminating OFAC knowledge to all of its ACH-originating customers. Dissemination of OFAC information needs to go beyond requiring "originators of ACH payments in their contracts with ODFIs to acknowledge that the ACH system may not be used to conduct transactions that are in violation with ... sanctions laws administered by OFAC...."¹³ The dissemination of OFAC information applies to all lines of business, especially those involving transnational activities.

Just as the Financial Crimes Enforcement Network (FinCEN) has pushed BSA compliance beyond the banking industry into other business sectors, OFAC compliance and enhanced customer due diligence should be pushed beyond banks and into all business sectors. A concerted effort to keep your customers informed of U.S. sanction programs can substantially reinforce your institution's frontline defense as your customers start to contemplate to whom they are providing goods and services (know your customer's customer).

7. Screen Cross-Border ACH

Contrary to domestic ACH, large ACH originators are filtering cross-border ACH transaction files. The OFAC risk associated with cross-border ACH is substantial because one or more of the parties involved in each transaction is not subject to OFAC's enforcement of U.S. sanction programs. Unlike domestic ACH practices, U.S. banks cannot rely on non-U.S. ODFIs for the screening of their ACH originators; nor can they rely on non-U.S. Receiving Depository Financial Institutions (RDFIs) for the screening of their ACH beneficiaries. Although the current volume of cross-border

ACH pales in comparison to domestic ACH, the screening of files is a daunting task. Screening live international ACH items presents many of the same challenges as its domestic counterpart. Of greatest concern: "Treasury believes that cross-border ACH transactions currently do not contain sufficient mandatory field information to permit an adequate degree of scrutiny of transactions for OFAC compliance."¹⁴ The National Automated Clearing House Association (NACHA) Rules Work Group #22 is in the process of addressing this issue by adopting new standards and formatting requirements that will include the name, address, and account number of each originator (and its client if the transfer is not from the originator's account); the name, address, and account number of each beneficiary; information sufficient to identify originating, intermediary, and beneficiary banks; and originator to beneficiary information (OBI) field specs identifying the purpose of each transaction.¹⁵ These new standards are likely to be adopted within the next two years and will go a long way toward creating an effective OFAC screening environment for cross-border ACH transactions.

In conjunction with NACHA, the Federal Reserve Bank's FedACH, in its role as United States gateway operator, has agreed to screen incoming cross-border ACH transactions. NACHA's future adoption of formatting requirements will enhance screening capabilities and also allow flagging of cross-border ACH transactions that contain potential OFAC violations.¹⁶ The receiving cross-border RDFIs will have to document their findings and the disposition of flagged transactions. Additionally, it is likely that the RDFIs will be required to report their findings to OFAC as the flagged transactions will be reported to OFAC by FedACH.

Screening of outbound cross-border transactions will still remain the complete responsibility of the ODFIs and their originators.

8. Screening Loans

In general, loans are considered low-risk transactions for OFAC violations. Most loan approval procedures utilize credit bureaus for the risk scoring process. Credit bureaus and negative database vendors have incorporated OFAC checks as standard service offerings. A simple check box on the loan application indicating that an OFAC check was reviewed on the credit bureau report prior to the loan funding process will suffice. If the loan is a revolving line of credit, regular OFAC screening is recommended periodically similar to any other existing account relationship. Again, the best practice for OFAC concerning existing accounts is to screen against every OFAC update within 24 hours. Lastly, logic would hold that an SDN would likely stop making payments upon discovering he or she was on an OFAC list.

9. Examine E-Banking Risk

OFAC monitoring for the e-banking environment, like all

transactional applications, should be based on a detailed risk assessment that focuses on the beneficiaries of the transactions. In most cases banks rely on their e-banking service providers for OFAC screening. Service providers are certainly in the best position to understand the scope of risk within the bank's e-banking network. Even though most banks rely on their service providers for OFAC screening, the bank is ultimately responsible, as there are no reliance provisions specific to e-banking.

Because the scope of the e-banking environment is very broad and will continue to evolve, it is necessary to understand the factors that can substantially change risk exposure in this area. Currently, the e-banking environment is predominantly domestic bill payment and relatively low risk. However, the scope of this business channel has huge potential to expand, and therefore the OFAC/AML risk could greatly increase.

Following are key elements to evaluate when assessing OFAC risk for e-banking applications:

- How extensive is your bank's e-banking network or service offering?
- Are transactions limited to a set group of established businesses or can payments be sent to anyone?
- Is the payment network domestic or global?
- Can you tell whether the local account holder's computer is physically in the United States or in Iraq?

It is vital for the OFAC compliance officer to stay up-to-date with the dynamics of this fast-changing service offering. At a minimum, banks should request documentation from their service providers regarding the scope of the services they have subscribed to, and records should be maintained regarding the service providers' interdiction capabilities and testing of those systems.

10. Monitor Stored-Value Cards

Stored-value cards, like all payment products, pose varying degrees of OFAC risk depending on the nature of the products. For example:

- A customer-only, low-value, non-renewable, domestic product poses very minimal OFAC risk.
- A noncustomer, open-loop, high-value product that is reloadable via a third party, includes duplicate cards, and has international access poses substantial risk.

OFAC monitoring for stored-value cards at the bank level has predominantly focused on screening card purchasers. This is especially important when providing this service to noncustomers. However, OFAC compliance for stored-value cards should go beyond just screening the purchaser or account holder and factor in a risk assessment of the card's potential use. Some stored-value cards can be used to facilitate anonymous transactions. These types of cards hold the greatest risk.

Here are the key elements to consider when risk-assessing any stored-value card for OFAC:

- Is it a payroll card?
- What is the monthly dollar limit?
- Are the cards reloadable? How many times in a month?
- Can the card be reloaded by a third party outside of the bank?
- Can the card be used outside the country?
- Does the bank have access to transaction reports from its service provider?
- Can the card be converted to cash or is it only for purchases?

Stored-value cards, like e-banking, have the potential to change quickly, so it is essential that OFAC compliance officers stay up-to-date with the dynamics of these products. Banks should obtain information regarding the interdiction capabilities of their service providers as well as reports for card transactions, OFAC filtering, and the testing of these systems.

Conclusion

This new era of OFAC compliance will be as ever-changing as U.S. foreign policy and regulatory enforcement. The banking industry will continue to be pressed ever harder to screen transactions and customer lists for the likes of terrorists and drug traffickers. While risk assessment and risk-based monitoring practices are crucial to these efforts, they are not standalone compliance practices. Risk assessment and monitoring must be interactive and managed in conjunction with sound OFAC compliance policies, ongoing training, and independent testing. Most importantly, each of these program elements must remain dynamic and be able to adjust to the ever-changing factors that influence OFAC program decisions—foreign policy, regulatory examinations, customers, product offerings, and filtering technologies, to name a few. BC

ABOUT THE AUTHOR

Timothy R. White, CAMS, is the national risk specialist for Banker's Toolbox, Inc., a leading BSA/AML solution provider for financial institutions. He is considered an expert on OFAC and has addressed OFAC and BSA issues at conferences throughout the United States. White is currently a member of a working group formed by the United Nation's Al-Qaida Taliban Sanctions monitoring team pursuant UNSCR 1735. In June 2006, at the request of the U.S. Department of State, he addressed an EU-US Workshop on Financial Sanctions and Terrorist Financing in Vienna, Austria. In 2005, he provided training for the Federal Reserve Bank's BSA/AML specialists on OFAC compliance technologies. In 2004, he was a member of the ABA's BSA-OFAC Working Group on OFAC Examination Procedures. In 2003,

he addressed BSA and OFAC as a faculty member of NACHA's Payments Institute. In 2002, White consulted the FBI on interdiction software capabilities within the financial institution marketplace. In 2001, while working for Thomson Financial Media, and in conjunction with First Data Western Union, he wrote the original product requirements for the first international interdiction database called Global Regulatory File, (now Accuity's Global WatchList™); the first commercially marketed international sanctions database. White is a member of the West Coast AML Forum Committee and is an active certified member of ACAMS first graduating class. After earning a Bachelors of Business Administration Degree (BBA) from the University of Iowa, he attended Xerox's International Management Center in Leesburg, Va. Reach him by telephone at (303) 757-1120 or via e-mail at timothy.white@bankerstoobox.com.

Endnotes

- ¹FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (July 28, 2006).
- ²Bank Secrecy Act Examination Manual, January 1996, BSA Work Program 103 Financial Record Keeping and Reporting Regulations, Anti-money Laundering Examination Work Program Advisory # 17, Division of Bank Supervision Board of Governors of the Federal Reserve System, Contained only the following five basic questions on OFAC Compliance:
 - Does the institution have policies and procedures in place for complying with OFAC laws and regulations?
 - Does the bank maintain a current listing of prohibited countries, entities and individuals?
 - Is the information disseminated to foreign country offices?
 - Are new accounts compared to the OFAC listings prior to opening?
 - Are established accounts regularly compared to current OFAC listings?
- ³U.S. Treasury procedures release for examining OFAC compliance (js2620.htm) (June 30, 2005).
- ⁴FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (July 28, 2006), Page 140.
- ⁵FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (July 28, 2006), Appendix K.
- ⁶FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (July 28, 2006), Appendix M and Matrix B published in 31 CFR Part 501 Federal Register (January 12, 2006). Partial withdrawal of proposed rule 68 Fed. Reg. 4422-4429 (2003) Economic Sanctions Enforcement Procedures for Banking Institutions.
- ⁷Sidebar: Hank Grant & Associates.
- ⁸FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (July 28, 2006), Page 138.
- ⁹Department of Justice, National Drug Intelligence Agency, National Drug Threat Assessment 2006, Appendix A.
- ¹⁰FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (July 28, 2006), Page 140.
- ¹¹Bank Secrecy Act Examination Manual, January 1996, BSA work program 103 Financial Record Keeping and Reporting Regulations Anti-Money Laundering Examination Work Program Advisory # 17.
- ¹²FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (July 28, 2006), Page 140.
- ¹³Department of the Treasury FAC Ref: GEN 155913, March 20, 1997.
- ¹⁴Department of the Treasury GEN 235613, November 9, 2004.
- ¹⁵Department of Treasury GEN 235613, November 9, 2004.
- ¹⁶Department of Treasury GEN 235613, November 9, 2004.