

International Wire Transfer Monitoring and What It Means to Your Bank

David DeMartino
Vice President, Metavante Risk and Compliance Solutions
Prime Compliance Suite

Because of the well-documented connection between international wire transfers and terrorist financing, fraud, and money laundering, the U.S. government has increasingly put these types of transactions under a microscope.

This was demonstrated by the recent revelation about the relationship between the U.S. government and the Society for Worldwide Interbank Financial Telecommunications (SWIFT), a consortium of 7,800 banks worldwide, in which the government was receiving information on millions of transactions per day processed through SWIFT's network.

But this also will intensify the pressure on the banking community as it relates to international wire transfer monitoring.

Why SWIFT transactions are so important to intelligence organizations

SWIFT is certainly the most prominent of all international wire transfer networks, and the richest resource for gathering information on international wire transfers.

Obtaining information on these transactions provides the government with the ability to detect global terrorist financing patterns. Wires that leave Saudi Arabia destined for Iran, or wires that leave Kuwait destined for Syria are on the SWIFT network, if the banks involved are SWIFT members. This provides the ability to connect the dots between sender and receiver in worldwide transactions, which in turn of-

fers valuable intelligence for the detection of criminal activities.

The big question is whether SWIFT will continue to provide these transactions to the U.S. government. Given the public exposure it received and the fact that SWIFT represents a worldwide community of banks, SWIFT may cut back on participation in this program. Only time will tell. But where does that leave U.S. banking institutions that conduct international wire transfers?

What the regulators will expect

The popular belief is that regulators will increase scrutiny of banks that deal in international wire transfers.

Most banks simply do not have a keenly focused approach when it comes to dealing specifically with wire transfers. Certainly manual or semi-manual processes will not work, and without the use of some type of detection technology, it is very difficult to establish the complex linkages required to detect suspicious wire transfer activity. Proven technology exists in the market and has for some time now – at affordable price points for even the smallest of banks – and the regulators are aware of this.

Know your customer's customer

The expectation is that you know your customer's customer. This applies in instances where a bank is participating in a correspondent banking relationship. Suspicious activity monitoring and detection is just as critical for these correspondent transactions, where the ultimate beneficiary is not the sending bank's actual client.

Regulators expect that you can correlate the relationship between all parties in a transaction, which when linked, can detect questionable activity.

The recommended approach

With or without continued government scrutiny of SWIFT transactions, the pressure for accountability rests squarely on the shoulders of banks that transact international wire transfers. It is in the best interest of these organizations to create the highest degree of protection by performing the following tasks:

- Conduct periodic vulnerability assessments to locate gaps in your compliance programs. A good third-party consultant should understand industry trends and match your risks against regulatory expectations and the actions of your peer firms.
- If you are a U.S. branch of an international bank, perform your due diligence in respect to both your correspondent banks and to the clients of your head office.
- If you are already using automated anti-money laundering (AML) detection technology to monitor wire transfers, then you need to put an upgrade process in place. Vendors are releasing new versions of their software, which contain new tactics and rules to detect suspicious activity in wire transfers. Not keeping abreast of these changes could result in missing a critical transaction that results in criminal activity.
- If you are monitoring using manual or semi-manual processes or system reports, etc., then you must consider automated AML detection technology. These systems are quite capable of detecting wire transfers that involve money laundering, fraud, and terrorist financing.

Planning and preparation today will affect the ability to grow your business tomorrow. By following the guidelines stated above, you should be well on your way toward protecting your firm from the perils of criminal activity and the wrath of the regulators.

For more information, contact David DeMartino at ddemartino@primeassociates.com.

2006 Bank Secrecy Act / Anti-Money Laundering Examination Manual (“Expanded Manual”)

Tony Kaus, CAMS
Risk & Compliance Specialist
Metavante Consulting and Professional Services

The Federal Financial Institutions Examination Council (FFIEC) manual, made available in June of this year, provides updated information about Bank Secrecy Act (BSA) anti-money laundering (AML) requirements. The purpose of the release is to provide additional information in support of a successful AML program and clarification about current regulatory expectations. The manual also:

- Employs a format change in which headings demonstrate how topics relate to one another
- Uses the previous manual’s overview style while including the relevant examination procedures within each section
- Provides hyperlinks in the electronic file, easing the ability to jump to a related page referenced within a section of the manual

The manual is a must read for anyone involved with BSA and USA PATRIOT Act compliance. The format, details, definitions, and examples used are clear and concise. The material provides comprehensive explanations in areas such as:

- The two-step process for risk assessment
- New required details for replying to a request letter (the letter received from the financial institution’s regulator four to six weeks prior to an exam)

- International transacting requirements (with timely discussion about Section 312a requirements)
- How to keep an AML program current

One notable characteristic of the expanded manual is the subtle supposition that software automation is being used to meet regulatory requirements. There are references to the identification of and request for lists of information by customer, channel, transaction, and many other category types. This is an aspect of examination that many banks report taking weeks to complete without automation – and that’s before an exam even begins. Electronic transactions are being scrutinized more closely than ever, and this goes beyond just wire transfers. There are many ramifications involving electronic transfers such as ACH, any cross-border payments, stored value cards, and more.

While most small institutions consider themselves insulated from money laundering, terrorist financing, trade finance, and 312a requirements or other international activities, the reality is that due diligence is expected for any customer activity, and customer activity at any institution can include any or all of these variables.

The new manual provides excellent detail and addresses several new topics. There are subtleties that must be scrutinized, but overall it is straightforward, clear, and concise, and it should be a significant aid to institutions of any size in the effort to implement and maintain a good AML program.

Metavante conducted a webinar on Tuesday, October 17, to present an overview of the expanded BSA manual. If you or someone you know would like to obtain materials from the webinar for a review of the expanded manual, please call 1-800-822-6758 or e-mail your request to Sales@Metavante.com.

ERA Provides Solutions to Operational Risk Challenges

Although banks have always been concerned with risk management, the nature of risk has evolved. Risk management has been transformed by globalization, consolidation, and realtime information. Its magnitude has been heightened by complex regulatory and legislative rules. This includes the Sarbanes-Oxley Act, which requires internal control reviews across most of a bank’s departments, as well as the Basel II Accord, which requires international banks to show they have sufficient capital set aside for emergencies and encourage safer banking practices through internal assessment processes and a transparent disclosure process.

In response to the new set of requirements and business pressures, banks have been compelled to re-evaluate their approach to assessing, predicting, and mitigating risk. Which means this “new” risk is an integrated concern with roots in the entire organization. Banks must now pursue a comprehensive, enterprise-wide approach to risk identification, evaluation, and containment.

Metavante offers specific technology, the Enterprise Risk Assessor, to help banks in this risk identification, evaluation, and containment process. We help institutions with a solution that can:

- Address Basel II requirements for risk reporting
- Support comprehensive operational risk management programs
- Track loss events
- Manage and document financial controls for SOX and FDICIA

- Manage and document the risks and controls surrounding the privacy requirements of the Gramm-Leach-Bliley Act
- Organize and document compliance assessments
- Serve as a system of record for internal audit

Operational risk has caused management to take a proactive approach to all risk management because it makes business sense. This motivation goes beyond avoiding the payout of regulatory penalties and fees. Exposure to risk can cause a loss of business momentum and revenue growth, reputation, and credibility.

To learn more about Enterprise Risk Assessor, [click here](#).

COMPLIANCE NEWS

Threshold for the Requirement to Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds

June 16, 2006

Article Summary:

The Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury and the Board of Governors of the Federal Reserve System (Board) are reviewing the threshold in the rule requiring banks and nonbank financial institutions to collect and retain information on funds transfers and transmittals of funds. FinCEN is reviewing the threshold in the rule requiring banks and nonbank financial institutions to transmit information on funds transfers

and transmittals of funds. The requirement to collect, retain, and transmit information on funds transfers and transmittals of funds applies only to funds transfers and transmittals of funds in amounts of \$3,000 or more. FinCEN and the Board request comment from the public, including law enforcement and financial institutions, to assess whether the potential benefit to law enforcement of a lower threshold outweighs the potential burden to financial institutions.

For more information, visit:

<http://www.federalreserve.gov/boarddocs/press/bcreg/2006/20060616/attachment.pdf>

Frequently Asked Questions - Conducting Independent Reviews of Money Services Business Anti-Money Laundering Programs

September 22, 2006

FinCEN has issued this guidance to assist money services businesses in understanding the regulatory requirements regarding conducting independent reviews of their anti-money laundering programs.

For more information, visit:

http://www.fincen.gov/Guidance_MSB_Independent_Audits9-21.pdf

FinCEN Issues Guidance on Suspicious Activity Reporting Requirements for Mutual Funds

October 4, 2006

FinCEN has recently issued guidance designed to assist mutual funds in complying with their suspicious transaction reporting requirements. According to FinCEN, under a final rule, mutual funds must file

reports with FinCEN that identify and describe transactions that raise suspicions of illegal activity. The requirement to file Suspicious Activity Reports (SARs) applies to transactions occurring after October 31, 2006.

For more information, visit:

<http://fincen.gov/newsrelease10042006.pdf>

LATEST NEWS

First American Bank Selects Metavante Risk and Compliance Solutions

MILWAUKEE, Oct. 9, 2006 — Metavante Corporation today announced that First American Bank, a full-service bank chartered in Illinois with more than \$2 billion in assets, has chosen a comprehensive suite of products from the Metavante Risk and Compliance Solutions division to automate its compliance with the Bank Secrecy and USA PATRIOT Acts. Metavante is the banking and payments technology subsidiary of Marshall & Ilsley Corporation (NYSE: MI).

Metavante will provide First American Bank with software and services from its Prime Compliance Suite, including: BSA Reporter, EDD Reporter, OFAC Reporter, Legal Reporter, the Prime Compliance Databank, and implementation services. First American Bank will use these tools in its ongoing efforts to comply with U.S. and international regulatory compliance requirements.

“We were looking for innovative technology to help us meet our compliance obligations and protect our customers from fraudulent activity,” said Sara Savanelli, senior vice president, First American Bank. “Prime Compliance Suite offers a single system of

record and functionality to automate our customer identification programs, ongoing transaction monitoring, case management, and government reporting. These unique solutions not only will help us effectively and efficiently comply with the law, but also grow our business.”

Metavante Risk and Compliance Solutions provide an integrated suite of Bank Secrecy Act, USA PATRIOT Act, and OFAC compliance software products that enable financial services institutions to monitor their customer transactions for money laundering and filter and review their customers’ transactions for sanctioned party violations. It facilitates suspicious activity detection and automates filing of the necessary regulatory reports with the appropriate governmental agencies. In addition, it helps financial institutions comply with the USA PATRIOT Act through customer identity verification and recordkeeping, a review module that compares customer records with known or suspected terrorist lists, and risk-based modeling of customers.

BSA Reporter software provides Bank Secrecy Act compliant anti-money laundering (AML) functions, and EDD Reporter software delivers Enhanced Due Diligence (EDD) for “Know Your Customer” and customer identification program compliance functions. OFAC Reporter software offers heightened awareness of politically exposed persons and financial fraudsters on a global basis and helps meet mandates set by global sanctioning bodies, such as the U.S. Treasury Office of Foreign Assets Control. Legal Reporter equips financial institutions with automated subpoena and FinCEN 314a management, including research and reporting capabilities.

The Prime Compliance Databank provides critical regulatory, legal, and reputational due diligence data for the compliance software suite. It creates global sanctioned party data, as well as non-sanctioned party data from multiple countries around the world.

Metavante's data lists are designed to greatly enhance sanctions filtering efforts and integrate seamlessly with Metavante's applications. The data lists can be used with other products.

"We build long-term relationships with the goal of helping clients confidently demonstrate an effective AML program to their regulators," said Gary Refinski, executive vice president, Metavante Corporation. "Whether they use our suite of AML and OFAC software, our compliance consulting services, or some combination thereof, the solutions we offer our clients are tailored to their needs and unique to the marketplace."

To read the complete press release and learn more about Metavante's products and services, visit www.metavante.com.

Contact: Sam Baumgarten, Metavante Corporation
678-533-4861, sam.baumgarten@metavante.com

Contact Information

Metavante Risk and Compliance Solutions, Prime Compliance Suite:

120 Wood Avenue South, Suite 401
Iselin, New Jersey 08830
Tel: 732-549-1400
Fax: 732-549-4300

For sales inquiries, please contact:

David DeMartino
120 Wood Avenue South
Suite 401
Iselin, New Jersey 08830
Tel: 732-549-1400, Ext. 217
Fax: 732-549-4300
E-mail: ddemartino@primeassociates.com

For consulting inquiries, please contact:

Kanwal Sandhu
120 Wood Avenue South
Suite 401
Iselin, New Jersey 08830
Tel: 732-549-1400, Ext. 214
Fax: 732-549-4300
E-mail: ksandhu@primeassociates.com

About Metavante Risk and Compliance Solutions
Metavante Risk and Compliance Solutions assist clients in developing efficient and sustainable risk programs to identify and manage the seen and unforeseen risks inherent in today's financial services operations. By combining operational risk and compliance acumen, financial services expertise, and enabling technologies, Metavante helps clients reduce their risk management burden and grow their business. Offerings include solutions for: enterprise risk programs, business continuity and information technology recovery planning, information security and privacy, fraud detection and prevention, and regulatory compliance, including the Bank Secrecy Act, USA PATRIOT Act, Sarbanes-Oxley Act, and Gramm-Leach-Bliley Act.

For regular updates, please sign up at
www.primeassociates.com