An Eli Financial Publication

AML COMPLIANCE Alert

PATRIOT Act, Bank Secrecy Act, OFAC, NCCTs, Terrorism Financing and More

Vol. 3, No. 7 Pages 49 - 56 **July 2006**

In This Issue ...

- *Money Laundering Threats:*
  GROWING ML THREAT IS SLIPPING UNDER THE RADAR AND PAST THE BORDER. The **FATF** wants you to know about a looming menace to your AML efforts. Discover why your enhanced due diligence team may need to make nice with customs agents to tackle this threat.**(Page 50)**

- *Risk Management Tool:*
  THINK CUSTOMERS ARE YOUR ONLY SOURCE OF RISK? THINK AGAIN. Most financial institutions outsource at least one of their servicing responsibilities to vendors. If you've gotten lax about managing the risk involved with these relationships, reinvigorate your efforts with this comprehensive tool. **(Page 52)**

- *Security Tip Of The Month:*
  PLAGUED BY LOOK-ALIKE SITES? FOLLOW 5 ESSENTIAL TIPS FOR DISARMING FRAUDSTERS. You've all heard the horror stories of individuals getting duped out of personal account information - why let it happen to your customers? Set a net to catch phishers while keeping your customers safe. **(Page 54)**

- *Security Bonus:*
  SURVIVE A PHISHING ATTACK WITH THESE 3 REMEDIES. You've done everything you're supposed to do to fend off fraudulent activity, but the criminals still find a way to grab hold of your customers' information. These 3 steps start chapter 1 of your worst-case scenario survival guide. **(Page 54)**

- *Industry Notes:*
  NEW BSA/AML EXAM MANUAL EMPHASIZES EMERGING RISKS. Get a sneak peek at the major changes in FFIEC's 2006 exam manual. Good news: One revision spells out your foreign correspondent account responsibilities. **(Page 55)**

Reader Question

- **FOLLOW UP WITH QUESTIONS IF HELOC FUNDS FIND NEW HOME COUNTRY.** Mortgage fraud is becoming a favorite tool for money launderers. Check out this situation to test your savvy on handling a suspicious HELOC transaction. **(Page 51)**

CONTENTS

We welcome your comments and suggestions!

Alice Williams, MA
Editor-in-Chief
888-779-3718 x325

Frederick E. Curry III, JD, MBA
Consulting Editor
Deloitte & Touche

Amy Marchant, JD, MA
Managing Editor
888-779-3718 x353

MONEY LAUNDERING THREATS

Growing ML Threat Is Slipping Under The Radar And Past The Border

▶ ***These 13 red flag indicators can help you construct a roadblock to trade based laundering***

Global trade in merchandise and services now accounts for more than $11 trillion per year, and this growth of international trade has also opened a gaping vulnerability for the financial institutions that maintain the accounts of import/export companies and finance a significant amount of these goods and services.

Customs agents inspect less than five percent of all cargo shipments moving through their jurisdictions, leaving 95 percent of trade transactions open to the possibility of abuse by tax evaders and money launderers. Now the **Financial Action Task Force** (FATF) wants to help you shrink this dangerous criminal portal with its recent report "Trade Based Money Laundering."

"This is the first time the FATF has specifically focused on one method of money laundering since it started issuing typology reports in 1996, which indicates the growing threat," says **Kenneth L. Bryant, MSCJ, CPP, CFE, CRP, CAMS, COMP, AML, FCoI.,** managing director of **Bryant & Associates, LLC.**

To begin tackling this money laundering menace, add these 13 red flags to your suspicious activity watch list:

- Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice;
- Significant discrepancies appear between the description of goods on the bill of lading (or invoice) and the actual goods shipped;
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value;
- The size of the shipment appears inconsistent with the scale of the exporter of importer's regular business activities;
- The type of commodity being shipped is designated as "high risk" for money laundering activities. Examples include high-value, low-volume goods such as consumer electronics;
- The type of commodity being shipped appears inconsistent with the exporter or importer's regular business activities;
- The shipment does not make economic sense. For instance, a company uses a forty-foot container to transport a small amount of low-value goods;
- The commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities;
- The commodity is transshipped through one or more jurisdictions for no apparent economic reason;
- The method of payment appears inconsistent with the risk characteristics of the transaction, such as an advance payment for a shipment from a new supplier in a high-risk country;
- The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction;
- The transaction involves the use of repeatedly amended or frequently extended letters of credit; and
- The transaction involves the use of front (or shell) companies.

Even at first glance, you can notice that many of the red flag indicators rely on evidence — such as bills of lading and invoices — that doesn't frequently reach the hands of banking officials. But informed approaches to this growing threat can help you grasp the information you need to identify risks and begin investigations.

Key #1: Invest in enhanced due diligence training for a dedicated team. "I would say the most important tool in combating trade based ML is having a special investigative unit that knows and understands enhanced due diligence," advises Bryant. That way when any high-risk activity surfaces, such as an import-export company doing business in a high-risk jurisdiction, you have a unit in place to complete the detailed investigation that is required.

Key #2: Anticipate the activities of your customers. "As part of due diligence upon opening an account, we investigate any associates that a company may do business with," says **Martin Prego, CAMS,** senior vice

Money Laundering Threats, *continued on page 51*

Money Laundering Threats, *continued from page 50*

president and head of compliance for **Espirito Santo Bank** in Miami.

This effort includes collecting business contracts and sending bank representatives for site visits to ensure that associates are real corporations and not shells. You are in a better position to detect unusual trade transactions after confirming this information early in the account relationship.

Key #3: Open the lines of communication. One of the things that can make trade based ML such an insidious hazard is that investigations generally need to involve multiple agencies. Working together with customs agents, law enforcement and tax authorities is a crucial step in initially identifying laundering activities.

Editor's note: *You can download the full FATF report on trade based ML from* www.fatf-gafi.org/dataoecd/60/25/37038272.pdf. ■

READER QUESTION

Follow Up With Questions If HELOC Funds Find New Home Country

Question: We recently had a bank customer send $50,000 to the Philippines through a cashier's check. When we asked about the source of these funds, he provided documentation of a home equity loan from another institution. What type of due diligence would be appropriate for this transaction? Should we file a SAR?

Answer: There could be a logical and legal reason for this transaction. For instance, the customer could be sending needed money to his family in the Philippines and the home equity loan was his only available funding source. On the other hand, there is also the possibility of suspicious activity. Either way, you won't know until you do some further investigation.

"We are in a position today where it's unacceptable to execute a transaction for which we have doubts. If there is a doubt, then you need to dig further until you are convinced of the nature of the transaction," advises **Tara Van Raepenbusch, CAMS,** AML compliance manager for **Kaupthing Bank Luxembourg**.

Van Raepenbusch suggests beginning your investigation by asking the following questions to better ascertain the risk level of the transaction:

- Are the home equity funds going to an account in the client's name or a third party?
- Why is the customer not sending the funds directly from the lending bank? Why is he using a cashier's check?
- How is the customer going to pay back the loan? Will the funds come from cash, an electronic transfer from the customer or a third party?
- Is there a guarantor linked to the account?
- Was the home equity application complete and satisfactory? Did it include a declared purpose for the loan, repayment plan, credit scoring, documents supporting approval, etc.?
- Did you question the account holder about why he was sending funds to the Philippines? Is the explanation satisfactory and logical?

Once you have answered these questions, you'll be in a much better position to determine whether or not the transaction warrants further enhanced due diligence efforts. If you find that the customer has misrepresented the purpose of the loan or misused loan proceeds — actions that FinCEN identifies as fraudulent mortgage activity — then filing a SAR would be appropriate.

Don't overlook: Once the funds are sent to the Philippines, following up with the customer to ensure that he uses the loan as stated on the application will be nearly impossible, warns **Martin Prego, CAMS,** senior vice president and head of compliance for **Espirito Santo Bank** in Miami. "Any time significant loan funds leave our jurisdiction, it's a major red flag for me," he adds. ■

