

# AML COMPLIANCE

PATRIOT Act, BSA, FinCEN, Terrorism Financing, SARs, Risk Analysis and More



## In This Issue ...

### *Enforcement Hotspot:*

#### **Think You Can Put Off Stringent AML Controls On Pre-Paid Cards?**

The pre-paid card is becoming a choice vehicle for criminals. In order to strengthen your compliance efforts and close monitoring gaps in this arena, follow these guidelines. (Page 62)

### *Crime Trends:*

#### **Stamp Out Money Laundering By Colombian Cartels.**

Drug lords are raking in the cash because they've found a clever way to launder proceeds via the Black Market Peso Exchange (BMPE). Stop dirty money from passing through your clients' accounts by learning BMPE's telltale signs and honing your investigative skills. (Page 63)

### *Risk Management:*

#### **A Convicted Money Launderer Tips You Off.**

Don't neglect the liabilities a devious employee can inject into your operation. Here are strategies that a convicted money launderer — and former bank executive — conveyed to help you protect your organization from the stiff penalties hers faced. (Page 65)

### *Technology Spotlight:*

#### **Catch Crooks With Comprehensive Case Management Tech.**

While a strong case management system can help you maximize efficiency, minimize risk and document the appropriateness of your actions (or inactions) for regulators, it's not always easy to determine if your system is operating at its full potential. Use these five questions to determine if your current case management tool is meeting your operational needs and, if not, to educate you before your next solution purchase. (Page 66)

### *Investigation Tips:*

#### **Arm Yourself Against Wayward MSBs By Investigating Licensure, AML Controls.**

Don't fall victim to bad business tactics on the part of your money service business (MSB) clients — doing so will invite the kind of federal scrutiny you want to avoid. Instead, use the three tips below to control your bank's risk exposure and help enforce BSA standards. (Page 67)

## CONTENTS

*Enforcement Hotspot* .....62

*Crime Trends* .....63

*Risk Management* .....65

*Technology Spotlight* .....66

*Investigation Tips* .....67

*Editorial Page* .....68

We welcome your  
comments and suggestions!

**Stacie Majoria, MA**

Senior Editor  
888-779-3718 x325  
staciem@eliresearch.com

**John MacKessy, CAMS**

Consulting Editor  
FTI Consulting

**Kimberly Gilbert, MFA**

Managing Editor  
kimberlyg@eliresearch.com

## ENFORCEMENT HOTSPOT

# Think You Can Put Off Stringent AML Controls On Pre-Paid Cards?

## ► Experts say: "Don't wait!"

Open-system pre-paid cards present significant risks because of their potential for abuse by money launderers and terrorist financiers. The pre-paid card is becoming a choice vehicle for criminals, warns **Paul Silverstein**, executive vice president of **Epoch Data Inc.** and a leading anti-money laundering strategist.

**Take note:** The recent indictment of the Moola Zoola program manager may have lessons for AML/BSA watchdogs on the growing convergence of identity theft, fraud and money laundering.

**What happened:** A person or group used pilfered personal information to extract funds from bank accounts electronically, explains attorney **Carol Van Cleef**, partner at **Bryan Cave**. To cover the tracks, funds were transferred to a Moola Zoola card, and then to a second Moola Zoola card. Ultimately criminals withdrew the stolen money from ATMs in Texas and Russia, she continues.

The Moola Zoola case provides an excellent illustration of the electronic financial system's vulnerability to abuse, says Silverstein. You should never underestimate criminals' potential for creativity and ingenuity, he counsels.

### Avoid The Ambiguity Trap Through Personal Accountability

**Eli** investigated the specific threats of open-system pre-paid (or stored-value) general purpose cards, typically branded by a major payment network.

Many experts believe these cards are riskier than other types of stored-value cards because they are fairly anonymous and — in some cases — provide access to ATM networks and call for non-bank third parties' participation, explains **Stanley Sienkiewicz**, senior manager at the **Federal Reserve Bank of Philadelphia** and author of a recent paper assessing pre-paid cards' money-laundering risks.

Given points of ambiguity relating to these cards in the AML/BSA regulations, financial institutions can become confused about who is responsible for monitoring and reporting suspicious activity. Don't point fingers at other parties and declare that "based on FIFEC manual requirements, I am not responsible for pre-paid card transaction monitoring," Silverstein adds. Every party in the stored-value card food chain — including issuers, plat-

forms and providers — has a stake in protecting the card program, declares Silverstein.

Since your institution operates these cards from a large pooled account, Silverstein advises that you must ask yourself: who's monitoring the individual activity within the accounts — the loads and spends on the processor level?

Rather than solely reacting to regulators and regulations, banks should take a proactive approach to squashing financial system abuse by criminals, says Van Cleef. In addition to being accountable for transaction monitoring, banks need to make sure they are monitoring these speedy activities in real time. Once the money is loaded onto one of these cards in the hands of criminals, the funds are practically irretrievable, emphasizes Silverstein.

**Advice:** Since stored-value cards precipitate a large volume of activity, you must automate the transaction monitoring process and case management due diligence with effective technology to aid in uncovering unusual events or patterns of activity, Silverstein recommends.

In order to strengthen your compliance efforts and close monitoring gaps, follow these additional guidelines:

### Conduct Due Diligence On Your Partners

Banks should conduct adequate and on-going due diligence on their relationships with non-bank third parties, says Sienkiewicz. Know the products, services and business practices of the processor. Find out if the organization conforms to BSA/AML requirements. Due to recent BSA enforcement actions, the AML program requirement has been extended to nonbank issuers, sellers and redeemers of stored-value cards, including money services businesses, Sienkiewicz notes.

Banks also have an obligation to investigate and understand who the program manager is *before* turning over a bin of their cards to the company he runs, advises Van Cleef.

### Know Your Customer

Amid the commingling of roles as the electronic financial industry continues to grow, clarify with your partners who precisely is responsible for gathering information on the customer, Van Cleef says. If you leave KYC activities in

*'Cards', continued on following page*

## CRIME TRENDS

# Stamp Out Money Laundering By Colombian Cartels

► **Eradicate the Black Market Peso Exchange at your institution with these 3 tips.**

Drug lords are raking in the cash because they've found a clever way to launder proceeds via the Black Market Peso Exchange (BMPE). Stop dirty money from passing through your clients' accounts by learning BMPE's telltale signs and honing your investigative skills. Here's what you need to know:

### Suspect Casas De Cambio

Be on guard when you see any money moving through, to or from Mexican casas de cambio. Although these "casas" (currency exchange houses) are legal, it is well known that BMPE brokers abuse them.

**Why?** It's easier for drug dealers to get money into the banking system in Mexico, so they smuggle drug proceeds across the border, says **Tom Lasich**, senior asset recovery specialist with the Swiss-based **International Centre for Asset Recovery**, and former money laundering program

manager with the **Federal Law Enforcement Training Center**. (Recently, U.S. federal agents seized \$11 million from the Mexico-based **Casa de Cambio Puebla, S.A.** as part of a money laundering investigation.)

Once criminals get their funds into the banking system, they often move it around to disguise its source.

**Bottom line:** Any wires connected to a casa de cambio are highly suspect, warns Lasich. Even though there may be legitimate reasons for the account, you should think twice about doing business with Mexican casas, as well as those located in other, equally high-risk, Latin American countries. If you decide to proceed, apply elevated due diligence levels to the account (i.e., monitor it closely on at least a weekly basis) and be on the lookout for large volumes of fund transfers.

*'BMPE', continued on following page*

*'Cards', continued from previous page*

the program manager's hands, you must make sure that the program manager is acting in accordance with the law, she says.

Experts ultimately advise that banks don't leave observance of these practices completely in the hands of the third party — a lesson potentially gleaned from the Moola Zoola case. "I think that many banks will decide as a prudent matter that they want to know who actually has one of their cards," Van Cleef says.

### Practice Thorough Activity Monitoring

Pre-paid card activities you should be monitoring include:

#### Load Velocity

While some card issuers think that card load limits them from being susceptible to money laundering, this is simply not true, emphasizes Silverstein. Numbers add up quickly when criminals possess a large volume of relatively low-limit cards that they reload on an ongoing basis, he says. Since pre-paid cards are an easy way for lawbreakers to move money, in many cases cross-border withdrawals will have you reaching for the SARs, he says.

**Example:** Twenty cards are loaded with \$500 every day from a retail location, and withdrawn every day from an international ATM location. These transactions add up

to \$10,000 moving across the border in a single day, or more than a quarter of a million dollars in a month — a prime opportunity for an unmonitored money launderer.

#### Spends or Withdrawals

As part of your monitoring efforts, look for unique patterns and events that signal suspicious activity.

If someone loads a card in the morning and the balance is withdrawn in full the same day, you must ask: "Why would a customer do this? Why is this activity occurring at this location?" Silverstein offers.

Another way to halt criminal activity is to track how your card activity measures up with the activity recorded by your peers — otherwise known as retail base comparison, adds Silverstein.

Deploying effective and thorough transaction monitoring is key not only to stopping criminal activity, but also to managing the stored-value card business for profit through protecting it from abuse, Silverstein says.

Van Cleef predicts that as time goes on banks will take a much more active role in these card programs, potentially by hiring a program manager to run a program or acting as a processor rather taking the role of a passive, recruited bank partner.

**Resource:** Read Sienkiewicz's paper: "Prepaid Cards: Vulnerable to Money Laundering?" at [www.phil.frb.org/pcc/discussion/D2007FebPrepaidCardsandMoneyLaundering.pdf](http://www.phil.frb.org/pcc/discussion/D2007FebPrepaidCardsandMoneyLaundering.pdf). ■

*'BMPE', continued from previous page*

Exercise similar caution with other types of Mexican accounts. To help determine their legitimacy, investigate whether there are signs of true business operations, such as payroll transactions, adds Lasich.

**Don't overlook:** Drug funds don't exclusively enter the system through Mexico or casas de cambio, says Lasich. For example, legitimate businesses may allow drug dealers to wire money through their accounts. Therefore, to adequately protect your institution you must look for BMPE red flags even in the absence of casa de cambio involvement.

### Examine Funds That Ping-Pong Around The Globe

Another BMPE tip-off is when an unrelated entity picks up the tab.

**Alert:** A telltale sign of trade-based money laundering is when the checks, bank wires or money orders sent to pay for U.S. merchandise do not originate from individuals or businesses invoiced for the goods, but instead from third parties with no apparent connection to the transaction, advises *2007 National Money Laundering Strategy*.

**Example:** Once the money enters the system, say through a Mexican casa de cambio, it often gets moved around a lot to "pretty it up," reminds Lasich. In this layering process, the funds may bounce from a Mexican cambio to China, and then to London, before finally being used to pay for goods intended for Colombian businesses.

**Takeaway:** Attempt to determine whether the transactions you're seeing are based on legitimate business activities. Know that if Colombian businesses are paying for shipments through unrelated entities (e.g., a Mexican casa de cambio, a wire from China or another foreign country, money orders, cash,) then they are probably involved in BMPE, Lasich says.

### Be Alert To Fluctuations From Industry Norms

Knowing typical — and unusual — types of transactions for a given business will inform your BMPE investigation efforts. Start with a peer activity review.

**What to do:** At account opening, ask customers to describe their normal business practices and transactions, and then cross reference that information with peers' standard activity in that industry and jurisdiction, recommends **Lyndon Ford**, senior consultant at **Wolters Kluwer**. Your benchmarking efforts have a two-fold purpose:

1. Confirm that the customer is supplying accurate information to act as a basis for their activity profile, and
2. Get a feel for industry standards so you know what constitutes unusual activity.

**How?** Subscribe to trade publications specific to clients' industries to familiarize yourself with normal activity, says Ford. **Dun and Bradstreet** is one resource for industry publications.

Also, Find out if any of your board members (or advisory board members) have experience with the industry your client claims to be involved with, and, if so, tap into their knowledge, suggests **Patti Blenden**, president of SC-based **Financial Solutions**.

**Bottom line:** Arm yourself with as much industry data as you can. The red flag indicating BMPE may be very small — such as invoices with prices that are much higher than normal, or shipping costs that don't line up with normal rates, Blenden elucidates. Develop your industry instincts well enough, and you'll have a better chance of picking up BMPE-related fluctuations. ■

### Defined: Black Market Peso Exchange

The BMPE is the largest known money laundering system in the Western Hemisphere, responsible for moving an estimated \$5 billion worth of drug proceeds per year from the U.S. back to Colombia, says the *2007 National Money Laundering Strategy* report.

The scheme allows drug traffickers to launder their illicit proceeds by exchanging their dollars in the U.S. for pesos in Colombia without physically moving funds from one country to the other. Here's how it works:

- ◆ Money brokers act as intermediaries between the drug traffickers and Colombian business people.
- ◆ The Colombia-based peso broker generally works with a U.S.-based counterpart, who collects the dollars from U.S.-based drug dealers and finds a way to enter the funds into the banking system.
- ◆ The money brokers sell the dollars they buy from drug dealers in the U.S. to Colombian businesses.
- ◆ The Colombian business people, in return for the discounted exchange rate on dollar-based capital, provide pesos to the Colombia-based broker. The intermediary, after taking a cut, routes the clean money to the Colombian-based drug dealers to pay for their dollars.
- ◆ The U.S.-based broker, in typical fashion, transmits the drug dealers' dollars to the credit of Colombian businesses, which pays their invoices at U.S. companies.
- ◆ The companies that receive the payments then ship products (e.g., electronics, alcohol, tobacco, used auto parts) to the Colombian businesses. Shipments arrive in Colombia illegally, since the businesses have no documentation that they legally paid for the goods. ■

## RISK MANAGEMENT

# A Convicted Money Launderer Tips You Off

## ► Crack down on illicit employee activity by reigning in trust

You focus much attention on snaring external money launderers who may be abusing your bank's services, and rightly so. But don't neglect the liabilities a devious employee can inject into your operation. Here are strategies that a convicted money launderer — and former bank executive — conveyed to help you protect your organization from the stiff penalties hers faced.

**Advice:** Check up on your employees — no matter how much you trust them — and monitor your account placements to minimize the potential for internal fraud, stated **Lucy Edwards**, former vice president in **Bank of New York's** (BoNY) Eastern European Division, at the recent *moneylaundering.com* conference. Edwards and her husband Peter Berlin pled guilty in 2000 to a conspiracy to launder money through the bank — a whopping \$7 billion, Edwards confirmed at the conference.

**What happened:** Edwards and Berlin co-conspired to effect almost daily wire transfers to assist their Russian-based cohorts in evading Russian custom duties and taxes and circumventing Russian currency control limitations, according to the 2000 allocution hearing transcript. The money-transmitting scheme also facilitated another documented criminal activity: a \$300,000 ransom payment on behalf of a Russian businessman who had been kidnapped in Russia.

Edwards and Berlin helped route the funds out of Russia, and ultimately to third party accounts worldwide, through three BoNY accounts Berlin had established for laundering purposes, their testimony revealed. The BoNY accounts, opened in the names of three U.S.-based front companies, enabled access to money-moving software called micro/CASH-Register, according to court documents.

How was Edwards able to launder billions of dollars over several years without being noticed? "Basically you could get away with murder because you weren't checked," she commented when questioned at the conference. BoNY since has taken steps to correct the breakdowns that Edwards exploited to carry out her illegal activities, including senior management and compliance department approvals of customers using high risk products such as micro/CASH-Register. Read on for more tips to help put adequate controls in place to root out and stop any Edwards-like employees at your bank.

## Monitor Account Purpose And Ensure Proper Divisional Assignment

Edwards' husband, Berlin, opened the three accounts they used to launder funds in the retail banking division, said Edwards. If Berlin's companies had been legitimate enterprises, the associated accounts should have been established in the corporate or international banking sectors, since they were receiving frequent remittances from Russia, she explained. At the time, the retail banking division manually monitored transactions and therefore lacked adequate mechanisms to monitor the tremendous transaction volume on Berlin's accounts for suspicious activity, she said.

Even with stringent controls, you still can fail at managing your AML risk if you can't guarantee that your clients are in the right buckets, affirmed Rachel Raemore, an anti-money laundering compliance director at **Wachovia Corporation**, at the conference.

**Takeaway:** Don't allow customers to fly under the radar by hiding high-risk accounts where they don't belong. Be on red alert if an employee facilitates an account opening in an improper service area or neglects to move an account to an appropriate sector if its profile changes. Review your most active — and most profitable — customers for their risk factors and suitability for the business units in which they reside, reminds **John MacKessy**, managing director at **FTI Consulting**.

## Temper Employee Trust With Adequate Check-Ups

Overabundant trust was what Edwards routinely pointed to when asked how she was able to escape notice while laundering billions of dollars in the late 1990s. While she admitted she deceived and exploited the trust of her colleagues and managers, she also suggested that a more stringent and thorough review of the implicated accounts and transaction reports might have raised suspicions earlier.

**Example:** The proper BoNY authorities remained for some time unaware that Berlin — whose eventual three accounts Edwards managed — was her husband, Edwards related to conference attendees. Therefore, as a bank vice president, she was able to manage transactions on extremely profitable client accounts connected to "companies" in which she had a stake. Although she signed yearly

*'Employee Risk', continued on following page*

## TECHNOLOGY SPOTLIGHT

# Catch Crooks With Comprehensive Case Management Tech

► **Tip: Ask vendors for a trial run before paying licensing fees.**

When unusual activity pops up on your radar, the clock starts ticking — your time is limited to assess the case and investigate suspicious transactions before reporting back to the feds. Using case management technology can help by prioritizing your alerts, managing SAR-filing deadlines and eliminating the need to manually review exception reports.

While a strong case management system can help you maximize efficiency, minimize risk and document the appropriateness of your actions (or inactions) for regulators, it's not always easy to determine if your system is operating at its full potential. Use these five questions to determine if your current case management tool is meeting your operational needs and, if not, to educate you before your next solution purchase.

### Does It Reduce False Positives?

An important part of an effective case management system is its ability to eliminate the “noise” of false alarms.

**Problem:** All vendors will say their product reduces false positives (alerts triggered by non-suspicious activity) in your environment, but pinpointing a product that will succeed at filtering out unneeded alerts may take a little work.

**Solution:** Request a no-obligations trial before you pay a software licensing fee, and review the cases it produces to make sure that it works, advises **Dave DeMartino**, a vice president in risk and compliance solutions for Milwaukee, WI-based **Metavante**. The vendor should be willing to let you test drive a limited version of the soft-

ware to confirm its “proof of concept,” he adds.

If you do see recurring false positives popping up, give the vendor a chance to lay out a solution. Vendors should be able to tell you how to reduce these false positives within your system once the product has been lightly implemented, says DeMartino. If not, move on to a different product.

### Does It Prioritize With Peer Group Input?

To stop money launderers in their tracks you must prioritize — or score — your cases with precision. Proper scoring will help ensure you are assigning your most experienced case managers to the riskiest accounts.

**Good news:** You can avoid spending resources unnecessarily to build a scoring model; ask the vendor to supply you with case scoring best practices from your peer group, advises DeMartino. Rather than inputting your own algorithm, use what the vendor has developed through work with your peers, and then tweak it for your own environment, he says.

Using peer input in case scoring not only is efficient, but it also demonstrates that you're using risk management best practices, which is sure to get regulators' approval.

### Can It Remember The Past?

Your case management solution should make it easy to integrate research and access historical records. Why? When a client's out of profile you can quickly look up past suspicious activity, as well as keep your documentation organized in one area.

*‘Technology’, continued on following page*

*‘Employee Risk’, continued from previous page*

code of conduct statements, she did not disclose her marital relationship with her “client” Berlin, an association admittedly difficult to discern since they maintained different surnames but which was well known to many lower-level staff members, says MacKessy.

**Lesson learned:** Don't trust your employees too much. “Check and recheck and do your homework as a manager,” advised Edwards from the panel.

To manage the risk your employees can present, screen carefully, never neglect thorough background and reference checks and require employees to take vacations — which means someone else must monitor their accounts' activities, advised attorney **Mark Matthews**, partner at **Morgan Lewis**, who was on a conference panel with Edwards.

**Epilogue:** Many conference participants were eager to know how much money Edwards and her husband made off the \$7 billion they helped launder, and what consequences they faced after authorities discovered their activities.

Edwards reported in her session comments that they made “only about a million dollars.” According to the allocation transcript, the couple accepted approximately \$1.8 million in unlawful transaction commissions from 1996-1999.

As part of a plea bargain in exchange for cooperating with authorities, Edwards and Berlin each received five years probation and six months' home detention in New Jersey. Also, they must make restitution of \$685,000 to the **IRS** and pay fines of \$20,000 each, according to an article published last June in the *New York Times*. ■

*'Technology', continued from previous page*

**Tip:** Look for a system that permits you to attach electronic files, like emails and spreadsheets, to the record. That way when a case is under scrutiny, the investigator doesn't have to work to bring all the relevant information together, says **Paul Silverstein**, executive vice president of **Epoch Data, Inc.** in Melville, NY.

**Don't forget:** Proper record retention also requires you to date and time stamp all documents and communication — so look for a case management product that has not overlooked this crucial record-keeping component. Also, remember that record retention requirements include not only items identified in the SAR narrative, but also other documentation (e.g., Internet searches, due diligence reports, etc.) that was used to support the investigation and decision to file/not file a SAR. So look for a product that incorporates electronic filing of all case materials.

#### Can It Pick Up On Concealed Relationships?

Link analysis is a technology's ability to see connections between people where investigators cannot. And you want this capability.

**How it works:** Through scrutinizing patterns in data, link analysis helps make apparent discreet relationships among accounts, people and organizations that could be involved in money laundering.

This technique is vital to comprehensive investigations and demonstration of effective due diligence to reg-

ulators — so you want to have a system with this capability, remarks DeMartino.

#### Does It Centralize And Correlate Information?

If you would like a case management system that helps eliminate subjective approaches and redundant efforts, then consider one that has the ability to cut across the silos of various bank departments.

Alert generation and the subsequent case management steps shouldn't be individualized within a department and its personnel, cautions Silverstein. Instead opt for a solution that facilitates a standardized workflow process and acts as a central repository for research from all service areas, from wire transfers to credit card and ATM use.

Streamlining the approach in this way can help reduce duplicative investigative and reporting efforts across departments, which in turn will help cut overhead, Silverstein maintains.

**Benefit:** A centralized case management repository can ease the disruption caused by staff turnover, create a benchmark for investigator productivity and present an added safeguard by allowing more checks on employee work, says Silverstein.

**Bottom line:** Look for a case management tool that matches your business needs, helps you focus efforts on true high-risk cases, facilitates easy access to research and records and effectively deploys investigation personnel. ■

## INVESTIGATION TIPS

### Arm Yourself Against Wayward MSBs By Investigating Licensure, AML Controls

► **Use the "attitude test" to gauge MSB compliance efforts.**

Don't fall victim to bad business tactics on the part of your money service business (MSB) clients — instead, use the three tips below to control your bank's risk exposure and help enforce BSA standards.

#### Tip #1: Assess Attitude And Transparency

Look for transparency in the MSBs with which you're associating. **How?** Apply what many experts refer to as the "attitude test." You want to deal with agencies that work to correct lapses and improve security as quickly as possible, not ones that thumb their noses at best practices in transaction monitoring, cautions Attorney **Carol Van Cleef**, partner at **Bryan Cave Law Firm** in Washington, D.C.

Also, look for comments from MSB operators that signal intention to avoid the rules, advises **Patrice Motz**, executive vice president of **Premier Compliance**

**Solutions** in Denver, CO. If an MSB believes the BSA doesn't apply to its operation, take that attitude as a red flag that the MSB doesn't have the right mindset about providing financial services, Motz says.

**Helpful:** Ascertain MSBs' attitudes by asking the following questions, offers Motz: 1) Do they recognize the risk involved with money flowing through their operations, and are they concerned about it; 2) Do they make an effort to know who their customers are; and 3) Are they as careful as your bank is in monitoring customer transactions?

#### Tip #2: Measure Fulfillment Of BSA Requirements

Good intentions alone aren't sufficient. It's important to ascertain whether MSBs are actually playing by the rules.

*'MSBs', continued on following page*

'MSBs', continued from previous page

Take these steps, suggested by **Ross Crumlish**, vice president in BSA/AML compliance at Bethesda, MD-based **Chevy Chase Bank**, to help safeguard your operation:

- ✓ Investigate whether the MSB is registered with FinCEN.
- ✓ Verify state licensure (if the host state requires licensure for particular MSB)
- ✓ Determine whether the MSB has an AML compliance program and officer charged with carrying it out.
- ✓ Find out if the MSB has a sufficient process for identifying suspicious activity.

**Best practice:** More banks are helping to identify MSBs that are flying under the radar. To participate, first have your staff establish whether an MSB you have contact with is subject to licensure. If any are failing applicable requirements, report them to the proper state and federal authorities, filing a SAR when appropriate.

**Tip #3: Rate MSB Risk Factors; Ask For Licensure Documentation**

Finally, to fulfill your regulatory obligations, you also must calculate and address the risks that each MSB presents to your institution. **How?** Evaluate the strength of your KYC procedures on MSB accounts. Also, examine MSB transactions to ensure that they match up with business activities that are normal for the client, as you would do with any account, says Van Cleef.

**Remember:** Determine the necessary level of diligence by rating risk factors such as the MSB's business volume, customer profile and range of services, instructs Crumlish. **Example:** If the MSB provides only check cashing services to a narrow customer base, that firm will require less attention and due diligence than an MSB that offers a wide range of financial services, such as money orders and money transmission.

**Tip:** Before starting a relationship with an MSB, ask its representatives whether the company requires a license, and if so, if they have obtained licensure. If the MSB representatives maintain that their business isn't subject to licensure requirements, you may want to ask for a letter from the appropriate state banking department that confirms this, recommends Van Cleef. **Pay attention:** Some MSBs may answer your request for such a letter with a document penned by their legal counsel, instead of from the state authority, cautions Van Cleef. In this case, make sure you check the qualifications of the legal counsel to render such an opinion, she suggests.

**Bottom line:** Until a single federal agency takes responsibility for regulating the sector, banks will continue to be charged with overseeing their MSB client operations. Use the information provided here to inform your staff on MSB monitoring to further your risk management efforts — and help control MSBs attempting to buck the system. ■



**Editorial Advisory Board**

**Diane E. Ambler, JD**  
Partner, Kirkpatrick & Lockhart  
Washington, DC

**Robert Kim**  
Chief Relationship Officer, Banker's Toolbox  
Los Angeles, CA

**Breffni McGuire**  
Senior Analyst, Tower Group  
Needham, MA

**Patrice Motz**  
Executive Vice President, Premier Compliance  
Solutions  
Denver, CO

**Lawrence D. Ostrow**  
Vice President, STB Systems, Inc.  
New York, NY

**Paul Silverstein**  
Executive Vice President, Epoch Data, Inc.  
Melville, NY

**Carol Van Cleef**  
Partner, Bryan Cave  
Washington, D.C.

**Senior Editor:** Stacie Majoria, MA  
(888) 779-3718 x 325

**Consulting Editor:** John MacKessy, CAMS  
FTI Consulting

**Editorial Director:** Erin Lang Bonin, PhD  
(888) 779-3718 x 336

**Bulk Sales:** (800) 508-1316 x 2313

**Customer Service:** (239) 280-2383

**Fax:** (800) 779-3560

*AML Compliance Alert* is published by Eli Research, 2222 Sedwick Road, Durham, NC 27713. Subscriptions cost \$532. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought. Subscriptions are also available in e-mail PDF format. Bulk pricing available. © World copyright 2007, Eli Research

**WARNING:** Unauthorized photocopying or e-mail forwarding is punishable by up to \$100,000 per violation under federal law. Have information on copyright violations? Call us! We'll share with you 25% of the net proceeds of all awards related to copyright infringement that you bring to our attention. Direct your confidential inquiry to Mark Lydard, phone (800) 508-1316, fax (954) 827-0697, or e-mail markl@medville.com. Send address changes to: AML Compliance Alert, PO Box 413006, Naples, FL 34101-3006.

**AML001** **Subscribe Today!**

Yes! Enter my one-year subscription to *AML Compliance Alert* for just \$532 + \$19.95 S&H.

**Payment Information:**  Check Enclosed: \$ \_\_\_\_\_ (payable to NHS)

Bill my credit card  MC  VISA  AMEX  DISC Exp. Date \_\_\_\_\_

Acct. # \_\_\_\_\_ Signature \_\_\_\_\_

Bill me (please add a \$15 processing fee for all billed orders)  P.O. \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Organization \_\_\_\_\_

Address \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ ZIP \_\_\_\_\_

Phone \_\_\_\_\_ Fax \_\_\_\_\_

E-mail \_\_\_\_\_

*AML Compliance Alert*  
**New Hill Services**  
Dept. 1380  
Denver, CO 80291-1380  
Call: 1-800-472-0148  
Fax: 1-800-508-2592