A Tidal Wave of Risk on the Horizon:

Why Big and Small Businesses Face New Risks Simply by Getting Paid

By Robert Mazur

Based on my 27 years of experience as a federal agent investigating international money laundering cases and the subsequent 2 years that I have spent providing anti-money laundering compliance expertise to the private sector, I have a startling message for companies involved in a trade or business. ***YOU ARE ABOUT TO EXPERIENCE AN ASSAULT BY GOOD AND BAD FORCES INVOLVED IN THE WAR ON DRUGS.***

I make this prediction as a result of a unique perspective achieved by only a select few experts in the field of money laundering. Like many experts, I've conducted dozens of lengthy historical investigations of international drug money laundering organizations. Unlike many experts, (*as a result of long-term undercover assignments)* I was also a major money launderer for both Colombian drug cartel leaders and significant U.S. based drug organizations for five years. My undercover life gave me a unique first-hand perspective from a viewpoint normally only experienced by high-level drug traffickers and money launderers. During the past two years, I have continued to work closely with law enforcement agencies as an instructor and a litigation consultant in money-laundering related matters. At the same time, I have also worked closely with major corporations to aide them in establishing meaningful anti-money laundering policies and procedures.

In my view, several issues have rocketed into the twenty-first century and set the stage for a potential onslaught of problems in the business sector:

- The Black Market Peso Exchange (BMPE), an underground banking system that has flourished in North and South America for decades, has finally caught the attention of the "*Generals"* leading the troops in the war on drugs. Investigations targeting this underground banking system are dramatically increasing. Proof of the priority now being given to the BMPE is evidenced by recent hearings on Capitol Hill, advisories issued by law enforcement agencies, and news reports like the August 29, 2000, Washington Post article written by Karen DeYoung "*U.S., COLOMBIA TO CONFRONT LUCRATIVE PESO EXCHANGE"*.
- Many large and small-scale clients of U.S. manufacturers readily use funds filtered through the BMPE. Although these purchasers are sometime sophisticated front companies controlled by organizations involved in drug trafficking and money

laundering, they also include "legitimate" companies that have purchased U.S. dollars outside the official banking system for various reasons (*which we will address below).*

- More than ever, large scale drug trafficking and money laundering organizations are shying away from laundering their ill-gotten gains exclusively through a series of bank transactions. The exchange of drug proceeds for goods that can be sold throughout the globe has always been a significant money laundering technique employed by sophisticated criminal organizations, but this technique is now more popular than ever.
- The IRS and other law enforcement agencies recognize the power of an old tool designed to track transactions in the private sector. Rigorous efforts to enforce the filing of this weapon, Form 8300 (Report of Cash Payments Over $10,000 Received In a Trade or Business), are underway throughout the United States. To increase voluntary compliance relative to the filing of Form 8300, the government has devoted more resources to the prosecution and imprisonment of those who fail to file the form.
- Law enforcement agencies are renewing a broader based attack on those individuals involved in the hierarchy of large scale drug trafficking and money laundering organizations. Due to realities like the rebel control of more than half of Colombia and rampant corruption in recent Mexican administrations fostered by drug lords, law enforcement agencies are prioritizing investigations of the individuals who dictate the command, control and fortunes of drug empires. This means that investigations focused on the river of drug profits flowing between North and South America will occur more frequently.

Many trades and businesses operating in the U.S. are unprepared to manage two forms of risk that evolve from the issues noted above. One area of risk relates to failing to establish record keeping systems to report certain transactions (*regardless of their nexus to a crime)* via Forms 8300. The second area of risk is promoted when a company fails to establish an early detection system that will identify suspicious transactions and trigger an appropriate response within a company.

Your company needs to professionally manage this risk by identifying it and establishing an Anti-Money Laundering Compliance Program that will efficiently eliminate potential problems. This program can only be accomplished by:

1. Establishing a written policies & procedures statement that clearly:
    - Defines the problem
    - Identifies and explains the applicable law
    - Affirms senior management's commitment
    - Outlines your compliance program
    - Designates a Compliance Officer/Committee
    - Outlines a disciplinary policy for an employee's failure to adhere to the policies & procedures of your company
2. Conveying your policies & procedures through training
3. Establishing an effective record keeping system that identifies reportable and suspicious transactions
4. Periodically verifying and testing the record keeping system under the supervision of outside counsel

Failing to address these issues and managing risk can result in substantial fines, the forfeiture of bank accounts, the loss of a good reputation, the end of careers, and a significant loss of your freedom (*prison terms).* Just ask the 35 employees of 16 American businesses who were criminally charged last year at the conclusion of a 2-½ year undercover sting, *"Operation Cash-Back",* engineered by the IRS and several other law enforcement agencies. These 35 employees of primarily computer distribution companies, including Command Systems, Wescom, New Miami Wholesale, Nextel, Daisytek, L&M, SDA Systems, and SED, were indicted for their roles in ***failing to file Forms 8300*** and/or knowingly accepting proceeds of a crime with the intent to conceal or disguise the source of the funds (***Money Laundering).***

The government collected evidence used to prosecute these businessmen by dangling large sums of cash and non-depository checks (*the instruments of payment required to be reported via Form 8300)* as payment for goods. During recorded conversations, undercover agents posing as buyers of computer equipment asked businessmen not to file 8300 Forms, and informed them that the funds used to buy the goods were derived from drug trafficking. According to a government official involved in the operation, "unfortunately, not one of the businessmen we contacted turned our undercover agents away".

Although none of the companies that employed the 35 businessmen have been charged to date, that is not always the case. Many companies have been charged in the past when their employees have committed crimes while acting within the scope of their employment. It is important to note that, pursuant to the theory of "vicarious liability", acts or omissions of an employee are imputed upon a corporation. Some of the factors that affect the application of this theory include whether or not the act or omission was made:

- within the scope of employment
- at least in part, with the intended purpose of benefiting the corporation

It is important for employers to recognize that whether the corporation actually benefited from the act or omission is less important than the existence of a motive to do so. So, if an employee, regardless of their level of importance or authority, acts or fails to act within the scope of their employment, with the intent to benefit the company, the corporation will likely be viewed as having committed the conduct of the employee.

An excellent example of a corporate defendant being held accountable for the acts of its employees is the 1991 conviction of the Bank of Credit & Commerce International (BCCI). Because the government proved that employees of the bank acted within the scope of their employment by conducting transactions on behalf of drug dealers, the bank was charged criminally, paid a $550 million dollar fine, and ceased doing business. BCCI was the world's 7th largest privately held bank with more than $20 billion in assets. They operated approximately 450 branches in 72 countries.

In order to diminish the risks posed by accepting funds from tainted sources, your company must identify the "red-flags" that generally accompany what the government defines as dirty money. Once understood, the recognition of these "red-flags" should raise your company's anti-money laundering antenna and trigger a course of action defined within your written policies and procedures.

A major source of funds carrying "red-flags" is the **B**lack **M**arket **P**eso **E**xchange (BMPE). The BMPE is a sophisticated currency exchange process that can only be fully defined in a separate lengthy review, but simply stated, the BMPE is an informal banking system operated by independent brokers who have access to both U.S. dollars and Colombian pesos. Often times, these brokers have the capacity to swap large amounts of dollars and pesos because they develop trusted relationships with clients who fall into two categories:

1. SUPPLY CLIENTS: Clients who have large sums of U.S. currency, with a desire to exchange their dollars for Colombian pesos.
2. DEMAND CLIENTS: Clients who have large sums of Colombian pesos, with a desire to exchange their pesos for U.S. dollars.

Suitcases, containing approximately $2 million in cash, delivered in Detroit to undercover agents by Colombian traffickers.

Generally, BMPE Demand Clients are South American businessmen who evade the customary fees and taxes paid by law-abiding importers. When exchanging pesos for dollars through official channels, Colombian importers must pay:

- 8% bank fee
- 6% prepayment of sales taxes
- 7% - 25% importation tax

Furthermore, the Colombian government requires importers to submit importation documents to justify exchanges of pesos for dollars that are conducted through official channels. This leaves a financial "footprint" that enables Colombia's equivalent of the IRS to trace transactions and ensure the subsequent reporting of income taxes generated from the sale of the imported goods.

To avoid the web of fees and taxes incurred through official exchanges, many South American businessmen turn to the BMPE, where they can secretly exchange pesos for dollars for a minimal flat fee. Through BMPE brokers, the South American businessman ultimately receives currency or negotiable instruments that the broker acquires from Supply Clients. The source of the Supply Client's funds creates a major problem for those who use the BMPE.

Although there can be other sources of dollars for BMPE Supply Clients, let's venture a guess about who possesses a significant amount of U.S. dollars and also has an interest in exchanging that cash for Colombian pesos through some means other than official channels. If it took you more than a few seconds to say, "drug dealers based in Colombia" then your response was a few seconds slower than that of the world's law enforcement community.

Even though every U.S. dollar placed in the BMPE system doesn't come from a drug dealer, every recurring user of the BMPE system knows that the system is primarily fueled by dollars generated from the sale of drugs. That fact taints the funds of virtually every repeat customer of the BMPE.

When trying to manage risks that emanate from BMPE funds or funds from any potentially tainted source, it is important to recognize that simply restricting sales to companies based in Colombia is not likely to diminish your company's risk of receiving tainted funds. It is important that you realize that:

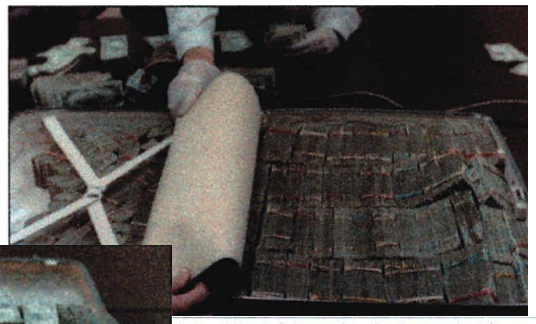
- Companies registered throughout the world use BMPE funds, not strictly companies based in Colombia.
- Drug trafficking organizations have become global players in the world economy.
- BMPE funds are paid to U.S. companies from client accounts controlled in cities throughout the world.

Have you or other employees of your company accepted payments from clients that bore any of the following "red-flags":

1. The customer's payments repeatedly included **"non-depository checks"** for no apparent reason. *(Non-depository checks are checks that are issued by an institution, rather than a check written on a personal or company checking account. Non-depository checks include cashiers checks, money orders issued by banks, postal money orders, travelers checks, bank drafts, payments issued by exchange houses – Casa de Cambios, etc. Although repeated payments with non-depository checks in any amount is a "red flag", repeated payments with non-depository checks issued for amounts under $10,000 are especially suspicious.)*

2. The payments received to satisfy the customer's account arrive in the form of checks or wire transfers from third parties or third party companies, rather than an account maintained in the name of the customer.

3. Checks received to settle an account contain one or more of the following characteristics:
   - Different typewriters or inks were used to note the date, amount, payee name or payer's signature on a check.
   - The typed amount on the check was covered by clear scotch tape.
   - The face of the check bore an unusual stamp, such as a small rabbit head, turtle, or insignia.



Left and Above: Suitcases from the photograph on the previous page demonstrating how drug money was packed. Mazur has received cash shipments in boxes, duffel bags, buckets, and just about any container imaginable.

4. Checks or wire transfers originating from jurisdictions that are considered by law enforcement authorities to be money-laundering havens. (*During the past two months, U.S. and other law enforcement authorities published advisories identifying fifteen nations that they claim are money-laundering hotspots. These nations are The Bahamas, Panama, Dominica, Cayman Islands, Cook Islands, Israel, Russia, Lebanon, Liechtenstein, Marshall Islands, Nauru, Niue, Philippines, St. Kitts and Nevis, and St. Vincent and the Grenadines. This list should not be considered as all-inclusive. Many other nations have been labeled by law enforcement authorities as money laundering havens that attract accounts controlled by criminals.)*

5. The customer maintains an excessive credit balance for no logical business purpose.

6. The customer makes repeated cash payments in increments less than $10,000.

7. The customer appears to structure transactions with your company in an attempt to keep single transactions in amounts under $10,000

8. The customer has no or limited business history in the industry, yet the customer proposes to conduct large transactions. These transactions may involve little or no credit.

9. The customer exhibits a lack of concern about transaction costs, the type of inventory acquired, etc. (i.e. Price or type of inventory acquired do not appear to be an issue.)

10. The customer appears to be acting as an agent for someone else and is reluctant to give details.

11. The inventory purchased appears to be diverted from the alleged end user to an unidentified third party.

12. The customer exhibits concern about secrecy (i.e. the filing of Form 8300)

13. The customer is the subject of law enforcement inquiry.

14. The customer is the subject of news reports or rumors of criminal activity.

There are certainly more than fourteen "red-flags", but those noted above should cause you and your company to pause and evaluate a client relationship. That evaluation, pursuant to your Anti-Money Laundering Compliance Program, may result in courses of action that either terminate a client relationship or document a due diligence process that supports the continuation of a business relationship. The bottom line is, it is very dangerous for you and your company to maintain a client relationship based only on a customer's ability to pay.

In a subsequent article, we will closely examine the "red-flags" that generally accompany funds that flow through the BMPE, and "red-flags" that generally accompany any funds that are associated with clients who may be making payments with money derived from an illegal source. In addition, we will review the legal theories used by law enforcement authorities to seize the bank accounts of business that have previously accepted criminally derived funds.

In the meantime, it is critical that your company reviews its Anti-Money Laundering Compliance Program and ensures that its employees are armed with the knowledge and resources needed to make their efforts in this area meaningful. The good and bad forces in the war on drugs are engaged in battle, and there are already enough victims without including an unsuspecting business.

Robert Mazur is the President of Chase & Associates, Inc., a company providing litigation support, consulting, training, and expert witness services. Mr. Mazur can be contacted at (813) 229-4542 or via e-mail, at bmazur@chaseandassociates.com