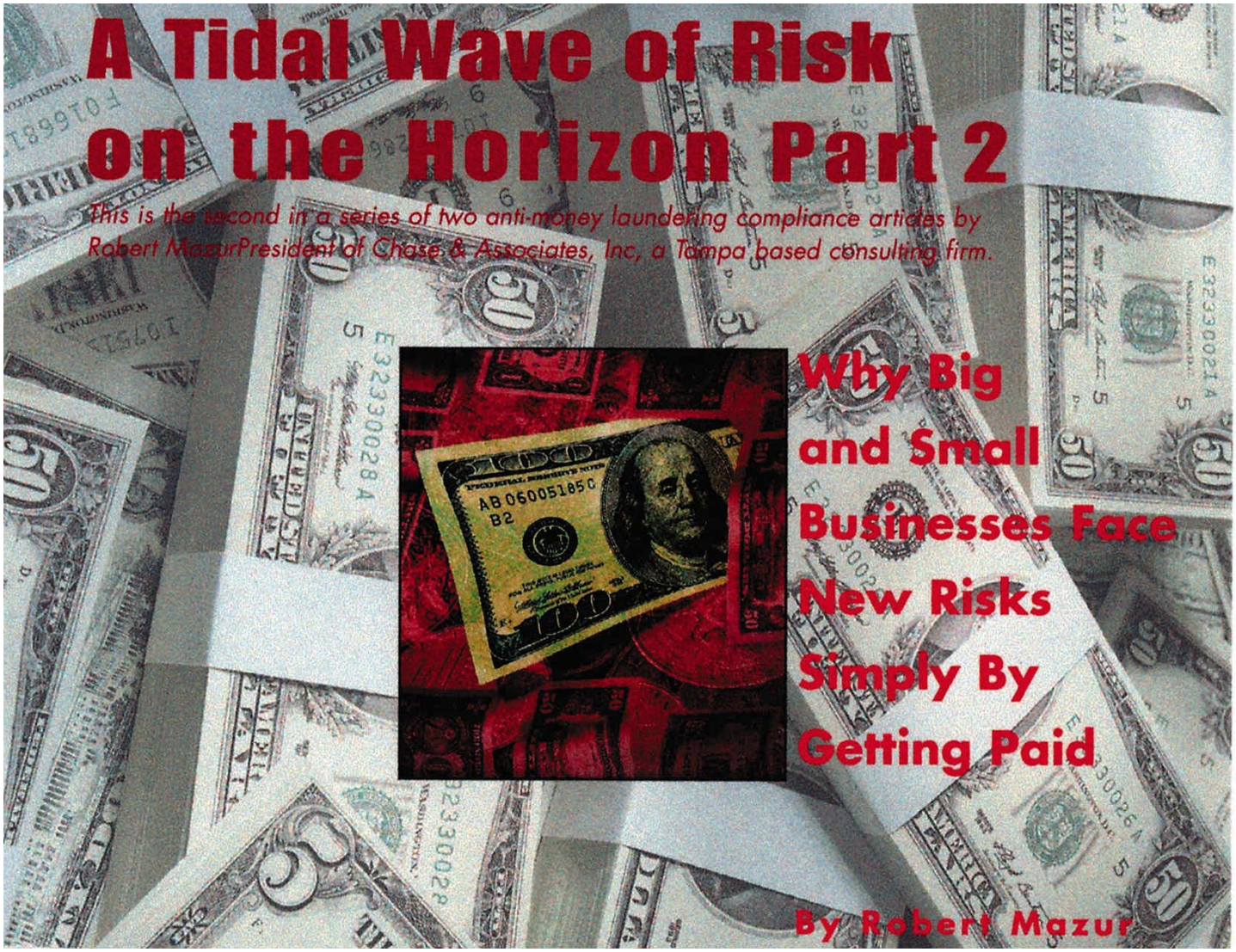

*Last month, Part I of this article addressed the threat posed to businesses operating in the United States by "**GOOD AND BAD FORCES INVOLVED IN THE WAR ON DRUGS".** We explained how drug traffickers, money-launderers, and buyers of drug dollars through the Black Market Peso Exchange (BMPE) are increasingly using tainted funds to purchase goods and services, rather than risk the web of anti-money laundering regulations established to monitor transactions in U.S. and foreign banks. We also noted that "big brother" has recently realized the impact of tainted funds on commerce and has declared war on individuals and businesses that knowingly accept funds from illegal sources. These and related factors create an increased challenge to credit managers and CFO's tasked with identifying and managing new risks.*

With increasing frequency, the media is publicizing "war cries" from leaders of the drug war, announcing their imminent attack on members of the private sector, including corporate giants in the tobacco, appliance, high-tech, and automotive industry. As recently as October 10th of this year, the front page of the New York Times forecasted warnings to U.S. businesses about the government's increased awareness that tainted funds are being dumped into the private sector at alarming rates. Lowel Bergman's New York Times article, ***"U.S. Companies Tangled in Web of Drug Dollars",*** should be required reading for any conscientious credit manager or CFO. The article not only summarizes the issues, but also notes that the seriousness of the problem has prompted recent meetings between Attorney General Janet Reno and corporate executives of many major U.S. companies, including Hewlett-Packard, Ford Motor Company, and Whirlpool.

This problem isn't a new threat to businesses in the U.S., because purchases of goods and services have been a dumping ground for significant amounts of drug proceeds during the past several decades. Frankly, the issue was substantially ignored, until recently. One contributing factor to the delayed initiative addressing issues like the BMPE is the prior unfamiliarity of some business leaders with the harsh reality that profits from the illicit drug trade pose a real threat to the corporate well-being of many legitimate businesses. A second contributor to this delay has been the slow evolution of the U.S. government's application of resources to this form of money

laundering. Now that the government is addressing this issue at warp speed, businesses have no choice but to pick up the pace and attempt to manage the risk created by the government's recent aggressive initiatives.

Like it or not, the laundering of tainted funds through purchases of goods and services occurs because of transactions conducted either wittingly or unwittingly. When they occur wittingly (with the knowledge of representatives of a business selling goods or services) the results can be devastating. A prime example of the devastation that can result from knowingly accepting funds from an illegal source will be announced in a Miami courtroom this month at the sentencing of Guillermo and Mauricio Schlaen. The Schlaens are two of thirty-five individuals who were arrested in South Florida at the conclusion of a Federal Undercover Operation known as ***"OPERATION CASH-BACK".***

Businesses have no choice but to pick up the pace and attempt to manage the risk created by the government's recent aggressive initiatives.

The Schlaen brothers were the owners and operators of A.G. USA Corporation, a company that distributed computer equipment in the Miami area. Individuals who claimed to be buyers of computer equipment contacted them in 1998. After these buyers (who were actually IRS undercover agents) placed their first order for an amount under $10,000, the agents began to explain details about their alleged business affairs.

During a series of recorded conversations, the undercover agents ultimately explained that they were acting as intermediaries for the Colombian Mafia, who supplied the funds that they were using to buy computer equipment from the Schlaens. The undercover agents subsequently delivered more than $10,000 in U.S. currency to the Schlaens on eight separate occasions, for the purpose of buying shipments of computer equipment ranging in value from roughly $12,000 to $36,000. As part of their pitch, the agents asked the Schlaens to not file IRS forms 8300, which would have otherwise alerted the government to each of the eight cash purchases in excess of $10,000. Without hesitation, the Schlaens agreed to the requests of the agents and accepted their money.

During one recorded undercover meeting, the Schlaen brothers were tasked with counting the cash that had been delivered by the undercover agents. While counting the cash, Mauricio Schlaen lost track of the count and jokingly commented that he must have been distracted by the smell of the money (meaning the latent scent of cocaine). The government used this and other statements to substantiate that the Schlaens believed that the money was derived from the sale of drugs. They were convicted by a Miami jury and face sentencing this month. Due to strict sentencing guidelines, they will live their next 3 to 3 ½ years behind bars at the expense of taxpayers.

Although the Schlaens actually received U.S. currency from the undercover agents in exchange for computer equipment, they could still have been charged with money laundering if the payments had been received in any other form, such as wire transfers from a business account. The key element in a money laundering offense is the knowledge that the individual had about the source of the customer's funds at the time of the transaction. If the seller of goods believes that their customer's funds (regardless of their form) represent proceeds from an illegal activity (in this instance drug trafficking) they can be charged with a money laundering offense, which is punishable by a maximum sentence of 20 years in prison.

Like it or not, the laundering of tainted funds through purchases of goods and services occurs because of transactions conducted either wittingly or unwittingly.

Although criminal convictions for money laundering require a unanimous finding by 12 jurors of guilt beyond a reasonable doubt, the government has other weapons used to attack money laundering which require a lesser degree of proof. These other weapons include the civil forfeiture laws that apply to the Money Laundering Control Act, Title 18 sec. 981. The Civil Asset Forfeiture Reform Act of 2000 (which became effective on August 23, 2000) made various procedural changes to the civil forfeiture laws. We will explore some of the procedural changes relative to civil forfeiture later in this article, but it is important to note that civil and criminal forfeiture laws are the tools applied by the U.S. government when they attempt to isolate their attack on the pocketbook of companies believed to have previously accepted funds that they knew, or should have known, were derived from illegal activity.

It is this theory that the government applied when they recently froze an account of Bell Helicopter, a company that sold a civilian helicopter to a Colombian "businessman" for $1.5 million. Because, among other things, Bell Helicopter received payment for the helicopter in the form of 31 separate wire transfers from accounts that had no ostensible link to any other or the aircraft's actual purchaser *(a red flag of tainted funds)*, the government claims that Bell knew, or should have known, that the funds used to purchase the helicopter were derived from an illegal source. According to news reports relative to this matter, the Colombian and U.S. governments claim that Bell's buyer in this instance is involved in drug smuggling.

As noted in last month's article, there are unique characteristics that are often associated with illicit funds. These characteristics, or "red flags", are not always evident because of the advanced sophistication of some money laundering organizations, but they can be associated with a good portion of the illegal proceeds that are tendered to U.S. companies. Being familiar with "red flags" is a front line of defense for a company that wants to avoid the type of legal proceedings confronting Bell Helicopter, as outlined above.

Red flags emerge from standard techniques used to launder illicit funds, and a series of "red flags" emerge from the money laundering technique known as *"smurfing"*. This technique was named after the little blue cartoon characters of the 1970's. It entails the use of large groups of apparent everyday people who work in concert to make thousands of cash transactions per day. Generally, a *"smurfing group"* is supervised by a manager who is responsible for converting millions of dollars in cash into either small cash deposits or purchases of small non-depository checks. *(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, and payments issued by exchange houses.)*

The key element in a money laundering offense is the knowledge that the individual had about the source of the customer's funds at the time of the transaction.

"Smurfing groups" ensure that their members make deposits or purchase non-depository checks in increments under $10,000 to avoid the Currency Transaction Reports (CTRs) that are filed by banks and Money Service Businesses (MSBs), such as Western Union, American Express, etc. *"Smurfing groups"* are so concerned about the filing of CTRs that they often make deposits and purchase checks in increments under $1,000. In recent years, many experienced *"smurfs"* have routinely purchased non-depository checks in small uneven amounts (i.e. $255.25) so their check purchases appear to be nothing more than an individual's purchase of a negotiable instrument that could be used to pay an electric bill.

It isn't uncommon for one *"Smurfing group"* to involve the efforts of twenty-five or more individuals. Each *"smurf"* generally starts their day with $50,000 or more in the trunk of their car and a map that identifies the various locations in their metropolitan area that offer the sale of non-depository checks. They drive to locations all day long, and exchange their cash for checks. At the end of the day, they deliver their day's work to their supervisor, and receive a small commission for their efforts (probably 1% or less of the total cash they converted to checks). These individuals are often illegal or legal aliens who have family members in Colombia. The continued presence of their family members in Colombia is considered collateral by the drug traffickers and money-launderers who employ them as *"smurfs"*. If law enforcement authorities catch a "smurf", the safety of the *"smurf's"* family members outside the U.S. is likely to be in jeopardy if they chose to cooperate.

The *"smurf"* may also open dozens of checking accounts in a given city. On a weekly basis, they may make several deposits under $10,000. More often, these deposits are made in increments under $1,000 to avoid drawing the attention of a conscientious bank employee. On a weekly basis, the *"smurf"* will write checks to a secondary account that is generally operated by a superior in the organization. This second account receives checks from accounts controlled by several *"smurfs"*. The operator of the secondary account (generally a supervisory member of the group) often writes checks to an account established in the name of an apparent business, and the checks drawn on the business account are either used to purchase goods or are sold to money brokers operating in the BMPE.

The Civil Forfeiture Reform Act of 2000 made various procedural changes to the civil forfeiture laws.

The pattern of transactions by *"smurfing groups"* potentially creates *"red flags"* when *"smurfed"* funds are tendered to a trade or business in exchange for goods. These *"red flags"* include:

- The customer's payments repeatedly include "non-depository checks"
- The customer makes repeated cash payments in increments less than $10,000
- The customer appears to structure transactions with your company in an attempt to keep single transactions in amounts under $10,000 *(This occurs for two reasons. The customer wants to avoid the filing of forms 8300, and "smurfed" funds aren't held for long periods of time in accounts. Significant balances don't generally accumulate in a "smurf's" account because the owners of the funds don't trust the "smurfs" with large balances, and these accounts are prone to seizure.*
- The customer's payments repeatedly include checks issued from several different accounts controlled by the same individual(s)
- The customer's accounts are paid with checks or wire transfers from third party accounts that have no ostensible link to each other or the customer.

Because *"smurfing groups"* realize that their pattern of transactions can draw attention when they are closely associated with purchases in the private sector, their non-depository checks and individual checks are sometime sold to money brokers who operate within the Black Market Peso Exchange (BMPE). Last month's article defined the BMPE and its elements. As noted in the prior article, BMPE brokers often collect cash from traffickers and money laundering organizations. These dollar funds are subsequently funneled into accounts of BMPE brokers who sell U.S. dollar checks to Colombian businessmen in exchange for Colombian pesos. Almost simultaneously, the BMPE brokers sell the Colombian pesos they acquire from "legitimate businessmen" to the drug dealers who have provided the broker with U.S. dollars.

When dollar checks are written by a BMPE broker to a client (often a "legitimate businessman" selling pesos) the checks issued by the BMPE brokers often bear certain unique characteristics *(red flags).* I have personally witnessed the consistency of these *"red flags"* throughout the past two decades.

Because BMPE brokers are concerned that a recipient of one of their checks may attempt to change the amount that appears on the check, they occasionally cover the numeric amount appearing on the check with clear tape. In addition, BMPE brokers often leave the date and payee blank when they tender their check to one of their customers. The date is left blank because the check may not be negotiated for a while. The payee is often left blank because the buyer of the check isn't always sure to whom he/she ultimately will tender the check in exchange for goods. Since the date and payee are often written on a BMPE check sometime after the amount and signature are noted on the check, BMPE checks often bear different colored inks or different styles of type.

Red flags emerge from standard techniques used to launder illicit funds, and a series of "red flags" emerge from the money laundering technique known as "smurfing".

Since BMPE brokers may operate numerous U.S. dollar accounts or trade numerous checks produced for them by related money laundering organizations, they occasionally (using a small rubber stamp) place a tiny insignia on the face of a check, thus verify that they are guaranteeing it will not be returned for insufficient funds. These small insignias can be in the form of animals (rabbits, turtles, etc.) or simply a unique shape.

Although BMPE brokers maintain accounts in banks within the U.S., some of their more significant U.S. dollar accounts are generally maintained in traditional "secrecy haven" countries (i.e. Panama, Cayman, The Bahamas, Switzerland, Liechtenstein, etc.) to enhance the anonymity of their role. Often times these haven country dollar accounts are maintained in the names of foreign "paper companies" that have no outwardly identifiable assets. In addition, BMPE brokers are often forced to maintain accounts in countries or territories where drug wholesalers exchange large shipments of cocaine for dollars (i.e. Dominican Republic, Puerto Rico, Mexico, etc.). To avoid the sometime risky physical transportation of dollars, the BMPE broker will maintain bank accounts and manage money-laundering groups that operate in these trans-shipment locations.

Due to the above-mentioned characteristics of BMPE checks, companies should be weary when:

- 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
- Checks received bear different color inks, different type settings, clear tape over the amount, or unusual small insignias imprinted by a rubber stamp
- Checks are issued from known money laundering jurisdiction(s) or locations commonly used as trans-shipment points for wholesale quantities of drugs
- Checks originate from a jurisdiction unrelated to the customer's business presence
- Checks are issued on accounts that appear to be "paper companies" established in haven countries known for bank and corporate secrecy

Other more readily recognizable *"red flags"* were identified in Part I of this article, which appeared in the October issue of Business Credit. The *"red flags"* identified in both this and the prior article should be reviewed to get a more comprehensive view of the overall *"red flag"* issues.

If one or more of the *"red flags"* noted in this and the prior article arise, you and your company should enhance your due diligence relative to the respective client. When these types of *"red flags"* accompany a client relationship, it is possible that the government may later suggest that, if you didn't realize that the customer's payments were made with illegal funds, you should have. On the other hand, if you enhanced due diligence and previously resolved questions concerning the client relationship, your risk will be dramatically decreased.

If the worst-case scenario occurs and the government seizes funds from your company's bank account, it is important for those charged with defending your company to be mindful of the Civil Asset Forfeiture Reform Act (CAFRA) of 2000, which recently

reformed provisions of the asset forfeiture laws. CAFRA went into effect on August 23rd of this year, causing a number of key changes. It is important to note that the new law imposes the burden of proof on the government, by "a preponderance of the evidence", to substantiate that the asset was used to commit a specific illegal act or represents the proceeds of a specific illegal act. The new revisions also note that, if a party claims to be an "an innocent owner" (such as would be the claim by Bell Helicopter in the case mentioned above) it is the claimant's responsibility to substantiate, by a preponderance of the evidence, that they were without reason to know of the illegal use or source of the property. If the claimant "substantially prevails" over the government and causes the seized property to be released to the claimant, the government must now reimburse the claimant for reasonable attorney's fees and costs. Prior to these revisions, it was less likely that a claimant would be able to recover attorney's fees and costs defending a seizure action taken by the government.

A sound Anti-Money Laundering Compliance Program is an inexpensive insurance policy against the tidal wave of risk on the horizon posed by tainted funds. This series of articles provides you with a roadmap to a meaningful plan of action that could prevent the unnecessary loss of company revenue, corporate reputation and personal freedom. The war on drugs has enough casualties without including unsuspecting businesses, so take the tools offered in these articles and reinforce your company's future.

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