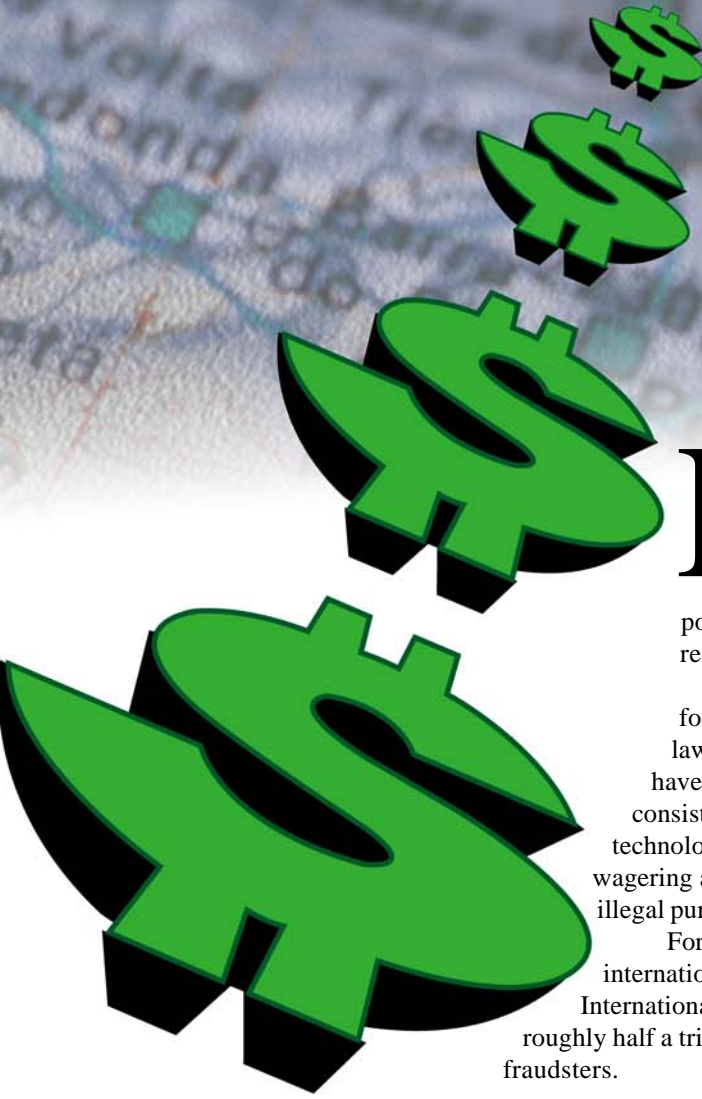


FOLLOW THE MONEY



NEW DIRECTIONS IN FRAUD INVESTIGATION

by Allan Nackan and Jonathan Cooperman



Readers of John Grisham novels may be familiar with the shady world of international fraud. In these fast-paced thrillers, corporate fraudsters go to great lengths to divert illicit funds to bank accounts, fictional corporations and suspect holding companies around the world. Yet, while Grisham postulates the possibility of his lone hero discovering and exposing these acts of fraud, in reality, fraud investigation is a tedious battle.

It was difficult enough in the days when fraudsters predominantly focused on hiding money offshore in jurisdictions with strict bank secrecy laws (such as Switzerland, the Cayman Islands, the Bahamas and other tax havens), but it is even more challenging today where financial transactions consist entirely of the movement of bits and bytes through sophisticated technological systems. Add to this the rise of online gambling and sports book wagering and we have new areas that can be used for money laundering and other illegal purposes.

For secured lenders, credit managers and other financial sector professionals, international fraud represents a disturbing, and growing, trend. According to the International Monetary Fund, between two and five percent of the world's GDP (or roughly half a trillion dollars) consists of money being laundered by international fraudsters.

(Continued on page 44)

Given the link between money laundering, organized crime and terrorist activities, it is critical for the financial services sector to work with experienced fraud investigators, forensic accountants and computer specialists to detect and track suspicious transaction patterns.

Staying aware of the risks

Financial services organizations must already comply with a range of legislation aimed at detecting and preventing fraud. Many financial institutions are required to report international electronic funds transfers that exceed a certain dollar threshold. They must report suspicious transactions, cross-border currency transfers and large cash transactions.

Despite these measures, fraud continues to rise for many reasons. Borderless global banking makes it easier to move funds from one jurisdiction to another. Round-the-clock access to the Internet can aid the fraudsters' ability to dissipate and hide assets offshore.

The prevalence of electronic online banking also complicates matters making international borders nonexistent. Historically, the bad guys had to physically visit bank branches to provide instructions regarding the transfer of funds. Today, electronic banking allows for the instantaneous transfer of funds without ever requiring those committing the fraud to travel or enter a bank branch. For example, an individual opened bank accounts in Switzerland to deposit funds from the safety of the same bank's office in another country — never having to set foot in Switzerland.

The anonymity of the Internet also facilitates the use of false identities to conduct transactions. The Internet has become a selling ground for shady financial institutions. And many scam artists brazenly advertise their services online.

International fraudsters often display unexpected organization and ingenuity. Some of the increasingly sophisticated schemes used to launder money include:

- Using "nominees," which are generally family members or friends, to conduct transactions on behalf of fraudsters.
- Using inconspicuous individuals, often called "smurfs," to deposit cash or buy bank drafts at various institutions for small amounts of money. Due to the size of these transactions, they rarely raise flags, allowing the crooks to surreptitiously

transfer these funds to a central account at a later date.

- Buying large assets, such as cars, boats and real estate, with cash, and later selling them to launder the proceeds.
- Using the proceeds of crime to buy foreign currency that is then transferred to offshore bank accounts.
- Smuggling funds across borders via mail, courier or other methods. Understanding the restrictive conditions of legitimate well-known wire transfer companies and ensuring transfers that meet these conditions can accomplish the fraudsters' objectives. Example: a fraud artist made sure each transfer did not exceed \$5,000, moving more than \$15 million over a period of time.

Real-world examples

This past February, Brazilian federal police arrested 55 people in a northern city who had illegally loaded keylogging software onto hundreds of computers. Keylogging programs copy the keystrokes of computer users and send the information — including passwords — back to criminals who can then assume a user's identity. In this case, the fraud ring stole approximately \$4.7 million from 200 different accounts at six banks before they were caught.

Similarly, in an article titled "Experts Issue Call to Arms on Online Fraud," published on July 25, 2006 by *The Sydney Morning Herald*, journalist Nick Miller reported that, last year alone, 80 million individuals' accounts were

compromised in the U.S. In one attack, scammers stole 145,000 records — including names, addresses, Social Security numbers and credit reports — from U.S. data broker ChoicePoint by posing as an authorized customer.

Consider the case of "Mr. D" who, in one of Canada's largest personal fraud cases, defrauded investors of more than \$75 million. By falsely stating he had the support of a large and credible organization, Mr. D convinced hundreds of individuals to invest in a bogus investment scheme. While more than \$6 million of valuable assets were purchased for his own use (in the names of family members and new corporations), close to \$70 million was transferred to online sports book-wagering companies in Costa Rica and Jamaica. Most of

Today, electronic banking allows for the instantaneous transfer of funds without ever requiring those committing the fraud to travel or enter a bank branch.



(Continued on page 46)

these monies were transferred back to different accounts in Canada, Switzerland and the United States, as well as used to purchase properties in numerous other jurisdictions.

Fraudsters also attract the attention of other fraudsters. It is common for fraudulently obtained monies to be moved through other individuals with a similar penchant to deal with, and launder, these illegally obtained funds, making tracing even more difficult.

Allan Nackan is a partner with the Toronto-based firm of A. Farber & Partners Inc. He can be contacted at anackan@afarber.com.



Recently, the entire online gambling and sports book-wagering industry has come under scrutiny. Billions of dollars of bets make the business lucrative and attract legal and illegal operators. The question of which of these activities are legal is the subject of much debate and the answers appear to depend on the jurisdiction where the activity occurs. This is difficult to determine when transactions are being conducted in cyberspace. In July 2006, a 22-count indictment against Internet gambling site BetonSports PLC (a public company in the United Kingdom) was issued in the United States on charges of racketeering, conspiracy and fraud. The CEO (a British citizen resident in Costa Rica) was arrested at the Dallas-Fort Worth airport and a warrant was also issued for the arrest of the Chairman. Allegations include failure to pay taxes on \$3.3 billion in wagers in addition to the illegal aspects of the activity itself.

Fraud is not limited to top-level corporate executives. A broad range of enterprising individuals now have the means and opportunity to engage in serious fraudulent activities that can potentially affect hundreds, and even thousands, of unsuspecting individuals.

Beating the fraudsters at their own game

Despite the sophistication of international scam artists, forensic accountants and fraud investigators and the computer specialists they work with are close on their heels. For instance, in situations where fraud is identified and there is an urgent need to preserve assets, affected parties can apply to a court for the appointment of a Receiver.

As officers of the court, Receivers have much broader powers than many realize. They can demand information and cooperation from many sources; seize physical and computerized records; and seize, preserve and sometimes even sell property funded by the proceeds of

crime. Receivers can also examine anyone reasonably thought to have any knowledge of the financial affairs of the fraudster.

To beat the fraudsters at their own game, investigators often use a combination of old-fashioned legwork and high-technology tools. Common strategies for uncovering international fraud include checking passports for evidence of visits to known tax havens, examining phone and fax records, reviewing credit-card statements and other mail, looking into a suspected fraudster's banking transactions and even checking the logs of couriers.

Investigators also rely on international online databases to track and uncover corporate fronts and affiliations and locate assets. Numerous computer forensic processes allow them to identify, collect, preserve and analyze computer-related evidence. And advanced techniques such as searching capabilities, email tracing and recreating deleted information also permit investigators to mine large volumes of electronic information to pinpoint patterns of suspicious transactions.

Using a combination of good intelligence and the element of surprise, Receivers, with their team of investigators, can often help to track hidden assets and recover funds. There are also extraordinary legal remedies that can be used to outplay the crooks. These include:

- ▶ Norwich Pharmacal Order, which is used to oblige banks to disclose relevant bank records without alerting the account holder;
- ▶ Mareva Injunction, which compels defendants to make full disclosure of their assets and allows for the freezing of worldwide assets;



Jonathan Cooperman is a partner with the Toronto-based firm of A. Farber & Partners Inc. He can be contacted at jcooperman@afarber.com.

-
- ▶ Anton Piller Order, which authorizes entry onto a defendant's premises to search for and secure property and evidence; and
 - ▶ Letters Rogatory, which allow a court in one country to request the assistance from the appropriate judicial authorities in another country.

The Interim Receiver in the case of Mr. D obtained an injunction and Letters Rogatory from the Ontario courts to secure assistance from the Costa Rican courts. After deploying a team to San Jose, the Receiver accompa-

(Continued on page 68)

Follow the money

(Continued from page 00)

nied police on targeted raids that helped the Costa Rican authorities obtain computer and other evidence that would be useful in the investigation of the flow of monies to that jurisdiction, and subsequently out of the country to other jurisdictions.

As an officer of the court, the Interim Receiver can bring legal proceedings to recover monies directly in the various jurisdictions. In the case of Mr. D, while most of these proceedings are civil, Switzerland allows criminal proceedings to be brought (at the request of the Interim Receiver) by the authorities to further recover illegal funds. The Swiss authorities can even allow the Interim Receiver to be involved in that process as a “partie civil.”



It's a small world, after all

As these examples make clear, instances of fraud frequently span international borders, making global cooperation increasingly important. In response to these concerns, a number of global initiatives exist to help deter, detect and prosecute fraudsters.

For instance, in 1989 the G-7 countries established the Financial Action Task Force (FATF) on Money Laundering. This intergovernmental body is focused on combating money laundering by enabling financial intelligence units to investigate the cross-border movement of funds. Several other international agreements also exist to help in this regard, including European Convention policies and a number of United Nations Conventions.

As fraudsters become more sophisticated, this type of international cooperation becomes more critical. By remaining aware of the warning signs of fraud, remaining diligent in their reporting duties and working in association with experienced forensic accountants, financial organizations can help to bolster these international efforts to stop fraudsters in their tracks. ▲

Note: Certain fact situations in this article have been altered to protect the integrity of a current engagement or litigation.