FINANCIAL CRIME IN INTERNATIONAL TRADE

Canada

EDC

Realize a World of Opportunity

ABOUT EXPORT DEVELOPMENT CANADA

WHO ARE WE?

Export Development Canada (EDC) is Canada's export credit agency. Our job is to support and develop Canada's export trade by helping Canadian companies respond to international business opportunities. We are a self-financing Crown corporation that operates at arm's length from the Government of Canada.

WHAT DO WE DO?

We provide insurance and financial services, bonding products and small business solutions to Canadian exporters and investors and their international buyers. We also support Canadian direct investment abroad and investment into Canada. Much of our business is carried out in partnership with other financial institutions and through collaboration with the Government of Canada.

HOW WE OPERATE

We are financially self-sufficient and operate much like a commercial institution. We collect interest on our loans and premiums on our insurance products. We also have a treasury department that sells bonds and raises money in global capital markets.

We are committed to the principles of corporate social responsibility. Our rigorous due diligence requirements ensure that all of the projects and transactions we support are financially, environmentally and socially responsible. We believe that adopting and embracing these principles while we facilitate trade for Canadian investors and exporters is good for business.

PARTNERSHIP IS OUR PREFERRED PHILOSOPHY

When we work on a transaction, we prefer to do it in explicit partnership with the private sector. We let the private sector player set the terms while we add capacity and share the risk.

TO CONTACT EDC...

Please refer to our Contact Us web page.

CONTENTS

This is an interactive PDF.

Click on any section in the Contents to link to the desired page.

Click to return to the Contents page.

Click to move forward or backward throughout the document.

Click to link to additional resources.

ABOUT THE GUIDE

This guide is designed to help Canadian exporters and importers learn how to manage the risks of financial crime in international trade. It has been written primarily for small and medium-sized companies, and in particular for chief executive officers, chief financial officers, legal counsel, heads of international sales and heads of international purchasing. Staff at other levels within your company may also benefit from the information contained in the guide.

DISCLAIMER

INTERNATIONAL FINANCIAL CRIME QUESTIONNAIRE: **ARE YOU AT RISK?**

Any Canadian company doing business abroad faces the risk of becoming involved in a trade-related financial crime, either as a victim or as an unwitting accomplice. Complete this quick questionnaire to see if your company may be vulnerable to criminal activities such as money laundering, terrorist financing, financial fraud or corruption.

ARE YOU INVOLVED IN MONEY LAUNDERING?

The purpose of money laundering is to disguise the source of money or assets derived from crime. It is intended to make crime-generated cash appear to be the proceeds of legitimate business activities, and a completely innocent company can become an unwitting accomplice to money laundering in several ways.

MONEY LAUNDERING BY A FOREIGN BUYER

To see if a **foreign buyer** may be trying to involve you in money laundering, consider the following questions:

- Is the foreign buyer trying to pay you through one or more apparently unrelated businesses in a third country?
- Has the foreign buyer overpaid you for a shipment of goods, and is now asking you to send the refund to an apparently unrelated business in a third country?
- Does the foreign buyer want to pay you in cash for a shipment of goods?

If you answered "yes" to any of these questions, you may be dealing with a money-laundering scheme. For more information, check out **page 17**, "If you're an exporter" and **page 20**, "What you should do."

MONEY LAUNDERING BY A FOREIGN SUPPLIER

To see if a **foreign supplier** may be trying to involve you in money laundering, consider the following questions:

- Is the foreign supplier asking you to pay for a shipment of goods by sending the payment to an apparently unrelated business in a third country?
- Is the foreign supplier offering you an exceptionally good deal that involves sending the payment to an apparently unrelated business in a third country?

If you answered "yes" to any of these questions, you may be dealing with a money-laundering scheme. For more information, check out **page 19**, "If you're an importer" and **page 20**, "What you should do."

ARE YOU BEING LINKED TO TERRORIST FINANCING?

Terrorist financing provides funds for terrorist activity and may involve funds raised from both legitimate sources and from criminal sources. Companies can become linked to terrorist financing schemes without any idea that this is happening.

Note that the money-laundering techniques outlined above can be used by terrorist organizations to move funds from one country to another.

To see if a **foreign buyer or supplier** may be trying to involve you in terrorist financing, consider the following questions:

- Are you being approached by a potential buyer or supplier who has been sanctioned by the Canadian government? ("Sanctioned" means that Canadian companies are legally prohibited from doing business with this person or organization.)
- Has a foreign buyer overpaid you for a shipment of goods, and is now asking you to send the refund to an apparently unrelated business located in a third country, and that third-country business is listed as a sanctioned entity?
- Is a foreign supplier offering you an exceptionally good deal that involves sending the payment to an apparently unrelated business in a third country, and that third-country business is listed as a sanctioned entity?

If you answered "yes" to any of these questions, you may be dealing with a terrorist financing scheme. For more information, check out **page 22**, "Sanctions and terrorist financing" and **page 22**, "What you should do."

ARE YOU A VICTIM OF FINANCIAL FRAUD?

If you're an exporter, financial fraud means you ship goods to a foreign buyer but don't receive payment for them. If you're an importer, it means you pay a foreign supplier for goods but receive either substandard merchandise or nothing at all.

FRAUD BY A FOREIGN BUYER

To see if a **foreign buyer** may be trying to defraud you, consider the following questions:

- Is the foreign buyer, who is in no obvious financial difficulty and appears to be functioning normally in its domestic market, refusing to pay for your goods even though there is nothing wrong with them?
- If the foreign buyer has provided a letter of credit (LC) to guarantee payment for your goods, is there any possibility that the LC may be fraudulent?
- If the foreign buyer has sent you a cheque to pay for your goods, is there any risk that the cheque may be fraudulent?
- If the foreign buyer has provided you with credit references, is there any risk that they may be fraudulent?

If you answered "yes" to any of these questions, you may be at risk of financial fraud. For more information, check out **page 23**, "If you're an exporter" and **page 26**, "What you should do."

FRAUD BY A FOREIGN SUPPLIER

To see if a **foreign supplier** may be trying to defraud you, consider the following questions:

- Is the foreign supplier offering you deep discounts for its merchandise, but only if you'll agree to a high-risk payment method (full or partial pre-payment for the goods, for example)?
- Has the foreign supplier shipped you inferior goods after you paid for quality merchandise, and is the supplier now refusing to replace the goods or refund your payment in a timely manner?
- Has the foreign supplier shipped you an insufficient quantity of goods after you paid for the full shipment, and is the supplier now failing to make up the shortfall or provide a refund in a timely manner?
- If a foreign inspection company has sent you an inspection certificate for goods you've bought from the foreign supplier, is there any risk that the either the certificate or the inspection company may be fraudulent?
- If you've bought goods from the foreign supplier, is there any risk that these goods may be counterfeit or may include counterfeit components?

If you answered "yes" to any of these questions, you may be at risk of financial fraud. For more information, check out **page 24**, "If you're an importer" and **page 26**, "What you should do."

ARE YOU BEING LINKED TO CORRUPTION AND BRIBERY?

Corruption refers to wrongdoing by government officials by means that are illegitimate, immoral or incompatible with ethical standards. Corruption in international trade is very often associated with the bribery of government officials.

To see if a **foreign buyer or supplier** may be trying to involve you in corruption and bribery, consider the following questions:

- Does the foreign buyer or supplier seem to be using business practices that would not be acceptable in Canada?
- Does the foreign buyer or supplier seem to be using business practices that would not be acceptable in its own country?
- Is the foreign buyer asking you to make a payment to a local official to gain preferential treatment in the local market?
- Is the foreign supplier asking you to make a payment to a local official before the supplier will ship the goods to you?
- In any of the situations above, is an agent involved in the transaction? (It is known that the use of agents is linked to a higher risk of corruption or bribery.)

If you answered "yes" to any of these questions, you may be risking involvement in the corruption of foreign officials. For more information, check out **page 27**, "Common bribery situations" and **page 30**, "What you should do."

INTRODUCTION

Could international financial crime endanger your company? If you're a Canadian exporter or importer, the answer is a definite "yes."

Financial crime in international trade is big business, with proceeds of up to $1.5 trillion annually. If you become embroiled in it, even by accident, the consequences can cripple your company financially and tear its reputation to shreds. This can be a very real risk, as two Canadian businesses discovered when they became involved in dangerous foreign markets. One paid fines of $9.5 million after being convicted in a Canadian court of corrupting a foreign government official. Another was convicted of bribery in an African court, paid fines of $2.2 million and was barred from doing business in the country for several years.

Cases like these show just how dangerous it is to ignore the risks of international financial crime. They also show that protecting your company against these criminal activities – which include money laundering, terrorist financing, financial fraud and corruption – can be one of the wisest investments you can make.

The most vital early-warning tool for identifying these trade-related crimes is the collective intuition of your company's senior management. Most senior managers, by dint of long experience, have developed a sixth sense that alerts them when something is not quite right about a business transaction. If this alarm is tripped, you shouldn't ignore it. Instead, start looking more deeply into the circumstances of the deal.

To do this, you should examine three key components of the transaction: the payment method it uses, the goods being bought or sold, and the counterparties[1] to the transaction. By diagnosing the situation in this way, you can determine what type of financial crime (if any) you are facing and what you should do about it.

[1] If you're importing goods, your counterparty is the foreign company from whom you are buying the merchandise. Conversely, if you're exporting goods, your counterparty is the foreign buyer to whom you are selling them.

CHAPTER 1: **RISKS AND RISK MANAGEMENT**

There are seven major risks related to international financial crime: counterparty risk, country risk, legal risk, financial risk, operational risk, reputational risk and agency risk. Your exposure to each risk will require its own assessment by your senior management, using assistance from outside experts as necessary.

International trade is so complex that eliminating every risk of financial crime is simply not a realistic expectation. A healthy dose of common sense, however, can help you cut your risks to an acceptably low level. Just keep the following in mind when you're looking at a potential business deal:

- **It looks too good to be true**

  If it looks too good to be true, it almost certainly is. If you're an exporter, your counterparty may offer wide margins and quick payment if you'll accept enormous risks related to the payment method. If you're an importer, your counterparty may offer heavily discounted goods if you pay in advance.

  In general, if a counterparty offers you a business proposition with unusually attractive terms or promises huge rewards for little or no risk, you should immediately suspect that something isn't quite right about the proposal.

- **You're judged by the company you keep**

  If you become associated with individuals or companies that have been involved in questionable transactions, your regular counterparties may become reluctant to do business with you and it may be hard to find new ones. Your financial institution may also question its relationship with your firm.

- **Keep it simple**

  Many fraudsters rely on complex transactions or confusing terminology to obscure what they are really doing. If a proposed transaction appears to be more complex than necessary, ask your counterparty why these extra steps or complications are needed. If the counterparty insists on them, ask yourself whether carrying on with the transaction is worth the possible consequences.

- **Do your homework**

  There is no substitute for due diligence. Any potential counterparty and any third party to a transaction may have ulterior motives, and the integrity of either may be questionable. You won't know unless you check.

With those basics established, let's examine each of the seven risks in detail.

COUNTERPARTY RISK

The location of your counterparty, its reputation and the history of your relationship with it are key factors in determining whether a transaction might become tainted by trade-related financial crime.

LOCATION OF THE COUNTERPARTY

You should take a very close look at any transaction with a counterparty located in a country that is notoriously corrupt, is in a state of civil unrest or is a known haven for narco-traffickers, organized crime, arms trafficking or other illicit activity (see also **page 11** on country risk). The probability of trade-related financial crime is higher in such countries and you should carry out much more rigorous due diligence when dealing with companies in these nations. This applies to every transaction with one of these counterparties – to allay suspicion, a criminally inclined counterparty may carry out one or more legal transactions with you before it tries to carry out an illegal one.

SANCTIONED INDIVIDUALS

The backgrounds of certain individuals who are part of an international trade transaction, such as the directors and shareholders of a counterparty, may indicate a high risk of criminal activity. Such people may also be sanctioned by the Canadian government and by recognized non-government organizations to which Canada subscribes (see also **page 22** on sanctions and terrorist financing). "Sanctioned" means that Canadian companies are legally prohibited from doing business with these persons or organizations.

Engaging in a business relationship that involves a sanctioned person or entity can inflict major damage on your company's reputation and may trigger criminal prosecutions in Canada or abroad against your company, its officers or both. Your best defence against this is to carry out very careful due diligence to determine whether anyone involved with a potential foreign buyer or seller has been sanctioned.

As an example, consider CIRC Systems[2] of Winnipeg, Manitoba. CIRC is considering a purchase of goods from Blackbeard Ltd., a company located in a central European nation that is experiencing a high level of internal violence. Groups engaged in this civil conflict have committed terrorist acts around the globe to bring attention to their cause, but Blackbeard itself seems to be a legitimate and harmless business.

Fortunately, the due diligence of CIRC's senior management reveals that one of Blackbeard's shareholders is associated with fundraising for a terrorist group, and the Canadian government has sanctioned this individual. As a result, CIRC immediately drops any idea of doing business with Blackbeard.

SANCTIONED ORGANIZATIONS

Organizations can also be sanctioned by the Canadian government, so your due diligence must ensure that your potential counterparty does not fall into this category.

Suppose, for example, that CIRC Systems receives inquiries from Blackbeard Ltd. about buying a quantity of relatively harmless goods from Canada. After carrying out due diligence, however, CIRC's senior management discovers that Blackbeard has been named as a terrorist organization and is listed as such in the United Nations Suppression of Terrorism Regulations. CIRC immediately ceases all contact with Blackbeard and informs the Royal Canadian Mounted Police (RCMP) of the situation.

[2] The examples using CIRC Systems are fictional. There is no such company in Canada.

CANADIAN TRADE AND ECONOMIC SANCTIONS

Canada has enacted legislation authorizing the imposition of trade and economic sanctions through the *United Nations Act*, the *Special Economic Measures Act* and some provisions of the *Export and Import Permits Act*. The RCMP and the Canadian Border Services Agency (CBSA) are responsible for enforcing these sanctions. For more information, refer to the Canadian Economic Sanctions page of the Foreign Affairs and International Trade Canada web site.

Note that trade and economic "sanctions," as covered in these Acts, are not the same as the "sanctions" applied under anti-terrorist legislation. The former apply to countries and include measures such as trade barriers, quotas and embargos. The latter are smaller in scope and are used to prohibit companies from doing business with specific organizations or individuals.

COUNTERPARTIES AND DUE DILIGENCE

There is no substitute for proper due diligence regarding your counterparty. You should always carry out – at the very least – the following checks on a prospective buyer or seller:

- What does a basic Internet search reveal about the counterparty?
- Does the counterparty have an established history of participating in similar types of transactions, or does it appear to be new to this kind of business?
- If it purports to have such a history, can it provide any references for the transactions in which it was involved?
- Can the counterparty direct you to any third-party analysts' reports about its business?
- Can you deal directly with the counterparty or must you deal only with its agent?

These queries are the most basic ones. You should use your experience in the international marketplace and your knowledge of your industry to ask many more questions. This will help you build a true picture of your counterparty risk.

COUNTRY RISK

Some countries present higher risks of financial crime than others. Nations mired in conflict, for example, may be associated with terrorist financing. Other countries are known for certain types of fraud. In still others, corruption is endemic in the financial sector and the government.

Before engaging in a transaction with a foreign company, you need to identify the risks of financial crime in the country where it is located. There are several sources of information that can help you do this, including the following:

- **Transparency International**

  Transparency International publishes the Corruption Perceptions Index, the Bribe Payers Index and the Global Corruption Barometer.

- **Financial Action Task Force**

  The Financial Action Task Force (FATF) is the world's most respected intergovernmental authority on money laundering and terrorist financing. It publishes a list of high-risk and non-cooperative jurisdictions.

- **Risk assessment providers**

  There are numerous risk-assessment firms that make their products available on subscription or as single purchases. One example is the Economist Intelligence Unit, which sells country reports that detail various types of risks associated with a nation's economy.

- **The Canadian Trade Commissioner Service**

  The Canadian Trade Commissioner Service, part of Foreign Affairs and International Trade Canada, publishes market reports by country.

You must also take country risk into account if your prospective counterparty is located in an offshore financial haven. In these places, banking secrecy is sacrosanct and local authorities have little desire to prosecute international business corporations operating from their shores.

LEGAL RISK

Legal risk pertains to the risk that your company's actions, or the actions of its officers, may breach the laws of Canada or another country. Such breaches can lead to criminal prosecution or actions in civil court. A firm can face financial penalties if convicted and individuals can face both imprisonment and fines.

FINDING LEGAL FIRMS ABROAD

These two web sites, among others, list legal firms around the world:

- International Financial Law Review
- Chambers & Partners

FINANCIAL RISK

If your company becomes embroiled in a trade-related financial crime, the costs can rapidly become very substantial. They may include one or more of the following:

- **Fines**

  A court or other public entity can levy substantial fines and/or penalties. If they are not paid, your firm can be driven into receivership.

- **External assistance**

  You may need to hire expensive external assistance, such as consultants and auditors, to remedy the situation.

- **System changes**

  You may be required to make expensive changes to your business systems to better manage the risks associated with trade-related financial crime.

- **Banking**
  Your bank may classify your firm as a high-risk client or may sever its business relationship with you entirely. This can force you to use more expensive banking services, since your new high-risk status will translate into higher fees and interest rates when you need credit to support your business operations.

Depending on the complexity and severity of the crime, the financial costs to a company can be crippling. In the worst cases, the damage may force the sale of the company or push it into bankruptcy.

OPERATIONAL RISK

A company's viability depends on a combination of healthy cash flow, production, inventory and sales. If a company becomes involved in a trade-related financial crime, these vital business operations will be placed in jeopardy.

- The company's cash, bank accounts and other negotiable instruments may be seized by the authorities. These assets may not be returned for a long time, if ever. This can severely undermine the business's cash flow and financial position.
- The company's physical goods, such as inventory and manufacturing inputs, may be seized. This will throw production schedules into disarray. As with the firm's financial assets, these goods may or may not be returned.
- The company's end products may be seized, which will make it difficult if not impossible to fill customers' orders. Again, these goods may or may not be returned.

STAYING VIABLE

EDC has several guides and resources to help you keep your company healthy. Among them are Credit Management Processes that Pay Off, Commercial Contract Terms and Risk and Cash Flow Management.

REPUTATIONAL RISK

A company's reputation for integrity is one of its most important assets. Maintaining this reputation should be a key priority for senior management, since it helps the firm attract good employees, loyal customers and the support of top banks. In contrast, companies with shoddy reputations not only tend to lose competent, honest staff, but can also attract dangerous customers who are seeking a business to use as camouflage for criminal activity.

A poor reputation for managing the risks of trade-related financial crime can also endanger a Canadian exporter's or importer's relationship with its financial institution. Under Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), individuals or businesses with a high risk of involvement in money laundering or terrorist financing, or who engage in trade with high-risk countries, can face much more rigorous due diligence and transaction monitoring by their financial institutions. The latter are acutely aware that if a client becomes involved in a financial crime, the institution itself can face punitive sanctions from Canada's financial regulators or from regulators in the countries in which it operates.

As a result, Canadian financial institutions with experience in international trade will often rid themselves of customers whose reputations suggest a vulnerability to financial crime, or an apparent willingness to overlook it.

AGENCY RISK

Many Canadian companies use agents or other local partners to act for them when buying and selling abroad. If the agent or partner engages in corruption and bribery to make sales or purchases on your behalf, you may not find out about it until too late – but you will still have to answer to the authorities and convince them that you were an unwitting party to the offense.

This hazard is often referred to as agency risk, and your first line of defence against it is due diligence. When choosing agents, be sure to find out whether they have ever been linked, even remotely, to criminal activities – not just to corruption, but to money laundering and terrorist financing as well. You should have formal procedures for vetting potential agents and you should follow these procedures rigorously.

The second safeguard lies in the way you communicate your needs to the agent. Your agency agreement should clearly define your ethical and business practices and your anti-corruption procedures and should include a statement that the agent understands them and will comply with them.

Third, you need to monitor your agents' activities for as long as they work for your company. This includes being able to inspect the agents' financial and commercial records relating to the business they conduct for you.

In addition, you mustn't inadvertently suggest to your agents that they can "do whatever is necessary" to generate business. If this misunderstanding leads to charges of corruption, the consequences can be very unpleasant for the Canadian company even if it was unaware (or maintained that it was unaware) of the agent's activities. One such firm was fined $2.2 million[3] by a court in an African country because its local agent bribed an official in that country. The Canadian company's defence, that it did not know about the payments, was rejected by the local court, and the company not only had to pay the fine but was also barred from doing business in the country for several years.

The United Nations Global Compact Office, in its *Business Against Corruption* guide, gives several signs that should warn you against hiring a particular agent:

- The agent has close family relationships with key official figures.
- The agent wants to be paid via a third party or an offshore bank account, or in cash.
- A person unexpectedly volunteers his services as an agent, apparently by coincidence, at precisely the time when you are running into unexpected difficulties in your negotiations.
- The agent is recommended by one of the government officials with whom your company is negotiating.
- The agent wants to remain anonymous.
- The agent wants to be paid large amounts of money in advance.

[3] All currency figures are in U.S. dollars unless otherwise indicated.

MANAGING THE RISKS OF MONEY LAUNDERING AND TERRORIST FINANCING

As mentioned earlier, the FATF is the world's most respected intergovernmental authority on money laundering and terrorist financing. The risk-based approach the FATF has developed is the most effective strategy that regulators can use to manage the risks associated with these two types of financial crime.

In 2007, the FATF published a report entitled *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*. While it is addressed primarily to financial institutions and public authorities, many of its recommendations can be relevant to Canadian companies doing business internationally.

Canada has its own financial intelligence unit, the Financial Transactions Reports and Analysis Centre (FINTRAC), which is an independent agency that reports to the Minister of Finance. It was established in 2000 and operates under the legislation and regulations set out in the PCMLTFA. FINTRAC has published a risk-based approach for entities that report to FINTRAC, such as banks, life insurance companies, casinos, real estate companies and accounting firms. Even if your firm isn't in any of these sectors, FINTRAC's suggestions may still be useful if you want to implement a risk-based strategy for dealing with financial crime.

According to FINTRAC, a risk-based approach to money laundering and terrorist financing involves the following activities:

- a risk assessment of the business's activities;
- risk mitigation to implement controls that will handle risks;
- keeping both client identification and, if required for the sector, beneficial ownership information up to date; and
- continuously monitoring financial transactions that pose higher risks.

Because the risks of financial crime are so varied, and the crimes themselves are often so complex, you'll need a range of strategies to manage your risk. These strategies fall into two categories:

- **Preventative strategies**

  Since an ounce of prevention is worth a pound of cure, you must develop strategies to avoid becoming involved in a financial crime in the first place.

- **Reactive strategies**

  You should establish strategies that will marshal your resources if you are about to be involved in a financial crime, or if you have already become entangled in one. You should have these strategies in place before any such situation presents itself.

Your preventative and reactive strategies should be embedded as policies and procedures within your firm, complete with clear delineations of responsibility for all staff who might help manage a crisis. In most cases, a combination of these strategies will prepare your company to deal with a financial crime if it occurs, or seems about to occur. If your company's resources in this area are limited, you should consider obtaining help from outside professionals.

CHAPTER 2: **MONEY LAUNDERING**

According to FINTRAC's definition, money laundering is the process used to disguise the source of money or assets derived from criminal activity. Because the proceeds of these crimes are so immense – estimated by FATF at $590 billion to $1.5 trillion worldwide each year – the money must be laundered in order to conceal its illegal origins from the authorities.

THE EFFECTS OF MONEY LAUNDERING

Money laundering encourages corruption and can destabilize the economies of susceptible countries. It also compromises the integrity of legitimate financial systems and institutions and gives organized crime the funds it needs to conduct further criminal activities.

It is a global problem, and the techniques used by its perpetrators are numerous and sophisticated. Technological advances in e-commerce, the global diversification of financial markets and the development of new financial products are providing many opportunities to launder illegal profits and obscure the money trail leading back to the underlying crime.

FATF RESOURCES ON MONEY LAUNDERING

The FATF has published several white papers about money laundering that are relevant to Canadian firms engaged in international trade. Two key ones are Money Laundering Vulnerabilities of Free Trade Zones and Best Practices Paper on Trade Based Money Laundering.

Although intended primarily for financial institutions and their regulators, these FATF papers can provide you with useful background information about the threats and techniques of trade-based money laundering.

THE MONEY-LAUNDERING PROCESS

While the techniques for laundering funds vary considerably and are often highly intricate, there are generally three stages in the process:

1. **placement**, which inserts the proceeds of crime into the financial system;
2. **layering**, which converts the proceeds into another form and creates complex layers of financial transactions (such as buying and selling goods, commodities or property) to disguise both the audit trail and the source and ownership of the funds; and
3. **integration**, which reinserts the laundered funds into the economy under a veil of legitimacy.

There are several common laundering techniques and new ones (or variations on older ones) are being developed all the time. The specific techniques used to manipulate a Canadian company depend on whether it is acting as an exporter or an importer.

IF YOU'RE AN EXPORTER

When you engage in an export transaction, you may become involved in money laundering through fraudulent payment methods such as indirect payment, overpayment and cash payment.

INDIRECT PAYMENT TO THE CANADIAN EXPORTER

A foreign buyer normally pays the Canadian exporter directly or sends the payment directly to the Canadian exporter's bank. If your buyer instead tries to pay you through an apparently unrelated business in a third country, you should examine the transaction more closely.

Consider again the example of Winnipeg's CIRC Systems. It ships a container of goods to Blackbeard Ltd., a buyer in central Europe, on open account terms. Blackbeard then tells CIRC that Yellow Co., a Caribbean company, will provide 60 per cent of the payment for the goods and Blue Ltd., located in Southeast Asia, will pay the 40 per cent balance upon successful shipment of the goods.

CIRC's management doesn't question why payment is being made in this piecemeal and indirect way. In fact, since both payments arrive in full and on time, the transaction is considered a solid one, which makes CIRC's sales team eager to do more business with Blackbeard. In the meantime, Blackbeard sells the goods imported from CIRC into its European domestic market, thus generating revenue in the local currency.

What CIRC doesn't know is that the payments from Yellow Co. and Blue Ltd. come from criminal activity in the countries where these companies are located.

The payment process is actually intended to launder the money and works like this:

- CIRC ships the goods to Blackbeard.
- Yellow Co. and Blue Ltd. send money to CIRC to pay for the goods.
- Blackbeard sells the goods into its European market, thus converting them into local, apparently clean cash.

Note that the goods themselves are of little importance, as they serve merely to camouflage the movement of the money. The real object of the whole transaction is to transmit value from the Caribbean and Southeast Asia to central Europe. Once in Europe, the transmitted value appears to be the result of legitimate business activity and Blackbeard can use it without fear of legal repercussions.

Moreover, because there are no obvious links from Yellow Co. and Blue Ltd. to the value that Blackbeard gets from selling CIRC's goods in Europe, investigators would need to follow the entire money trail in order to identify the criminal activity.

If you encounter a transaction such as this, which involves complicated payment arrangements and seemingly unrelated third parties, you may justifiably suspect that money laundering may be taking place.

OVERPAYMENT TO THE CANADIAN EXPORTER

Exporters are accustomed to receiving exact payment for their goods when payment is due. Overpayment by a foreign buyer is unusual and, while it may be explained by clerical or computer errors, there are cases in which it is deliberate and is actually intended to launder money.

Let's consider again the unfortunate CIRC Systems and its shipment of goods to Blackbeard Ltd. After invoicing for the amount due, CIRC receives Blackbeard's payment via wire transfer. The amount of the payment, however, exceeds the invoiced amount by a considerable percentage.

Shortly after CIRC receives the invoice, Blackbeard contacts the company and apologizes for the error. It then asks that CIRC refund the amount of the overpayment not directly to Blackbeard in central Europe, but instead to Yellow Co. in the Caribbean.

Thinking that it's Blackbeard's business where its sends its money, CIRC complies. By doing so, it unwittingly helps launder the proceeds of crime by disguising the origins of the funds received by Yellow Co. While they appear to come from CIRC, they are in fact coming from Blackbeard.

Money launderers are always seeking ways to distance cash from the criminal act that generated it. By using the overpayment technique, the launderer makes it appear that the wire transfer is a legitimate payment to the Canadian exporter for goods delivered. The payment thus escapes scrutiny and the launderer takes advantage of the Canadian exporter to move the excess funds to a third party in a different country.

CASH PAYMENT TO THE CANADIAN EXPORTER

Cash payments are unnecessary in international trade and suggest criminal activity. If a Blackbeard representative were to offer CIRC Systems a suitcase full of cash in payment for a shipment of goods, CIRC should immediately cancel the transaction and report the attempt to the appropriate authorities.

THE BLACK MARKET PESO EXCHANGE

In the late 1970s and early 1980s, narco-traffickers in Latin America were generating enormous amounts of cash by selling cocaine into the United States. Moving these dollars into the U.S. banking system and transferring them to Colombian, Panamanian and other banks, however, became difficult when the U.S. Drug Enforcement Administration (DEA) and U.S. Customs began investigating major money-laundering cases. Before long, mountains of cash began to pile up in the drug traffickers' safe houses.

At the same time, governments throughout Latin America were becoming concerned about runaway inflation caused by foreign borrowing to finance budget deficits. As a result, legitimate importing companies in the region were being faced with restrictions on currency trading. Many Latin American currencies were pegged to the U.S. dollar at artificial rates, so these importers faced a dilemma – to obtain the liquidity they needed to fund their imports, they could either buy scarce U.S. currency at the official government rate, or purchase it on the black market.

This established a classic supply-demand situation. On the one hand were narco-traffickers with U.S. dollars they wanted to exchange for the domestic currencies of their home countries. On the other were the importers, who needed to sell their domestic currencies for U.S. dollars, preferably outside the scrutiny of the domestic regulators who supported the artificially low U.S. exchange rates.

It was not long before a black market developed, with Latin American brokers arranging peso/U.S. dollar exchanges between importers and narco-traffickers.

Bankers, lawyers and accountants were all active in this lucrative market, which became known as the Black Market Peso Exchange. There were even cases of foreign exchange houses dealing in illegitimate transactions. For companies exporting goods to Colombia, for example, requests would occasionally be made by importers to accept cash payments or consigned bank drafts drawn on various banks.

Whenever the authorities uncovered a Black Market Peso Exchange, legitimate firms could face enormous losses if they had sold goods to importers who had purchased illicit currency from Black Market Peso Exchange brokers, as either the goods or funds could be seized by the authorities.

THE BLACK MARKET PESO EXCHANGE GOES GLOBAL

It has recently become clear that Black Market Peso Exchange transactions span the globe and are not exclusive to trade between the United States and Latin America. In December 2010, the U.S. Immigration and Customs Enforcement (ICE) arrested 13 people in Puerto Rico on money-laundering charges. According to the investigation, the defendants allegedly attempted to launder approximately $8 million, of which $4 million was seized by ICE agents.

The investigation also revealed that the defendants used the Black Market Peso Exchange to launder the illegal proceeds of drug trafficking organizations through electronic transfers to China, Hong Kong, Colombia, Sweden, Panama, Spain, the United Arab Emirates and the United States.

Although first identified several decades ago, the Black Market Peso Exchange continues to operate today and law enforcement officials describe it as one of the most successful mechanisms for laundering the proceeds of crime. A Canadian company can suffer considerable damage if it is found to be selling goods to a foreign buyer who has paid for them with dollars obtained from the Black Market Peso Exchange.

IF YOU'RE AN IMPORTER

As an importer, you normally pay for foreign goods by sending your payment either directly to the overseas supplier or directly to the supplier's bank. If the foreign company instead asks you to make the payment to an apparently unrelated third party, it may be trying to launder money.

Suppose CIRC Systems purchases goods from a central European vendor (our old friend, Blackbeard Ltd.). CIRC knows very little about Blackbeard, but the latter has offered a 25 per cent discount off its regular price for the goods, an offer that is too good for CIRC to refuse.

Blackbeard then asks CIRC to make payment via wire transfer not to Blackbeard itself, but instead to Yellow Co., a firm in a Caribbean country. Blackbeard's goods arrive at CIRC's warehouse and CIRC duly transfers the payment to Yellow Co., as requested.

What CIRC does not know is that it has become involved in money laundering. By using CIRC as an innocent middleman, Blackbeard has transferred the proceeds of its central European criminal activities to Yellow Co., which is controlled by Blackbeard's shareholders. Worse, the smoothness of the transaction has made CIRC eager to do more business with Blackbeard.

Transactions such as this are typical for international money launderers, since it can be relatively easy for them to conceal their activities within the enormous volumes of international trade. As in the above example, launderers may also be quite happy to sell their goods at a discount if it will induce Canadian buyers to pay for the merchandise in roundabout ways.

INDICATORS

The United States Department of Homeland Security has published a list of indicators that suggest potential money laundering. These indicators are extremely broad, however, and should be seen only as general guidelines. They include:

- payments to a vendor made in cash by unrelated third parties;
- payments to a vendor made via wire transfers from unrelated third parties;
- payments to a vendor made via cheques, bank drafts or postal money orders from unrelated third parties;
- false reporting, such as commodity misclassification and commodity over-valuation or under-valuation;
- carousel transactions (the repeated import and export of the same high-value commodity);
- commodities being traded that do not match the businesses involved;
- unusual shipping routes or transhipment points;
- packaging that is inconsistent with the commodity or shipping method; and
- double invoicing.

WHAT YOU SHOULD DO

If you suspect that a transaction with a foreign counterparty may involve money laundering, you should immediately do the following:

- Retain legal counsel to advise you how to proceed.
- Gather all supporting documentation and place it in a secure location.
- Notify both your financial institution and FINTRAC that the transaction may be related to money laundering.
- Do *not* tell your counterparty (or a third party, if there is one) that you have reported the transaction.

CHAPTER 3: **TERRORIST FINANCING**

Article 2 of the United Nations International Convention for the Suppression of the Financing of Terrorism defines terrorist financing as follows:

- Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
  - An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
  - Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

Canada has incorporated this perspective on terrorist financing into the PCMLTFA.

THE CANADIAN PERSPECTIVE ON TERRORIST FINANCING

According to FINTRAC's definition, terrorist financing has the following characteristics:[4]

- Terrorist financing provides funds for terrorist activity. It may involve funds raised from both legitimate sources and from criminal sources such as the drug trade, weapons smuggling, fraud, kidnapping and extortion.
- Terrorists use various money-laundering techniques to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. When terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult. The amounts associated with terrorist financing also tend to be smaller than is the case with money laundering.
- To conceal the movement of funds from Canada to countries where the money will be used to support terrorist operations, terrorists use international banking centres, various informal value-transfer systems such as hawalas,[5] and the physical smuggling of cash, gold and other valuables.

[4] This section is an edited version of the FINTRAC definition of terrorist financing.

THE FATF ON TERRORIST FINANCING

The FATF has published extensively on terrorist financing in white papers and other reports, including its *Guidance for Financial Institutions in Detecting Terrorist Financing*. This document may be useful to Canadian firms engaged in international trade.

SANCTIONS AND TERRORIST FINANCING

Your most effective defence against becoming embroiled in terrorist financing is to carry out rigorous due diligence. If you discover that your potential counterparty – whether an individual or a company – has been sanctioned by the Canadian government as a terrorist or a terrorist organization, you must immediately halt the transaction. You must also report the transaction and the business relationship to Canadian government authorities.

If your company sends a payment to a sanctioned individual or organization, or receives a payment from these sources, your bank's anti-terrorism safeguards will detect the transaction. The bank will then report the transaction to FINTRAC, the RCMP and the Canadian Security Intelligence Service.

Canada's banking regulator, the Office of the Superintendent of Financial Institutions (OSFI), provides a list of sanctioned individuals and organizations. Public Safety Canada has a list of entities sanctioned by Canada's *Anti-Terrorism Act*. Canada's Department of Foreign Affairs and International Trade publishes Canadian Economic Sanctions on its web site.

RESTRICTED AND CONTROLLED GOODS

The Canadian government places restrictions on how certain goods may be exported from Canada or imported into Canada. If your company deals in these goods, you must be aware of the laws and regulations related to them and your company should have procedures that reduce the risks of such commerce. If a potential foreign buyer asks you to provide such goods and you do so, you may be participating in a transaction linked to terrorist groups or to the proliferation of weapons of mass destruction.

The Canadian government agency responsible for regulating restricted and controlled goods is the Trade Controls and Technical Barriers Bureau. The Bureau's web site provides a variety of resources, including lists of restricted and controlled goods. The CBSA's web site has a guidebook where you'll find more detail about issues such as controlled exports and reporting requirements. Refer to Exporting Goods From Canada: A Handy Guide for Exporters.

Before starting a new business relationship with an overseas trading partner, you should always check the above lists to make sure the new counterparty is not sanctioned by the Canadian government.

WHAT YOU SHOULD DO

If you suspect that an individual or organization may be linked to terrorist financing, you should immediately contact the National Security Information Network of the RCMP. Send an email or telephone 1-800-420-5805.

[5] Hawalas are unregulated financial networks that transfer money across international borders.

CHAPTER 4: **FINANCIAL FRAUD**

If you're an exporter, financial fraud means shipping goods but not receiving payment for them. If you're an importer, financial fraud means paying money for goods but either receiving substandard items or not receiving the goods at all.

IF YOU'RE AN EXPORTER

You can substantially reduce your risk of not being paid for your goods if you can arrange payment in advance or have your buyer pay cash on delivery. However, foreign buyers are very unlikely to accept such arrangements. In international trade, it is normal for an exporter to ship goods to the foreign buyer and then wait for up to 180 days to receive payment. This exposes the exporter to various types of fraud, such as the following.

NON-PAYMENT BY THE FOREIGN BUYER

This happens when the exporter delivers the goods but the foreign buyer doesn't pay for them, even when the buyer is in no obvious financial difficulty and appears to be functioning normally.

AVOIDING FRAUD THROUGH CREDIT MANAGEMENT

You can reduce your risk of being defrauded by ensuring that you have effective credit management practices and that they include rigorous credit checks, especially of new customers. For more information, please refer to EDC's Credit Management Processes that Pay Off.

Consider again the example of CIRC Systems. Nine months ago, CIRC shipped a container of goods to Blackbeard Ltd., a buyer in central Europe, on open account terms. But despite numerous attempts, CIRC is unable to obtain payment for the merchandise. Repeated demands have not generated any reaction, yet CIRC knows that Blackbeard continues to operate and is importing goods from other suppliers and selling them in its domestic market.

Legal fees are high in Blackbeard's country and the judicial system is notoriously corrupt, so CIRC has little hope of obtaining payment. The company now faces a complete write-off of the shipment's value. It has thus been a victim of financial fraud in the form of non-payment, which it might have avoided either by a rigorous credit check or by shipping the goods only after payment was guaranteed (through an LC, for example).

Partial payment is a variant of this type of fraud. In this version, the foreign buyer pays a percentage of the amount due, sometimes in advance, but never pays the balance.Partial payment is not always a form of financial fraud. It can also be a commercial response to short shipments or damaged goods received, for example. For more information, refer to our **Risk and Cash Flow Management** guide to reduce your commercial risks in doing business internationally.

FINANCIAL FRAUD USING TRADE FINANCE PRODUCTS

Most Canadian companies engaged in foreign trade are familiar with the trade finance products offered by the financial industry, such as LCs and documentary collections. These products are well entrenched in the Canadian marketplace and many companies use them to reduce their risk of non-payment in international trade transactions.[6]

Unfortunately, trade finance products can also be manipulated for criminal purposes, so you should always obtain them from a reputable financial institution with a proven record in international business. If you don't, you may substantially increase the probability of becoming a victim of financial fraud through means such as the following:

- **Fraudulent LCs**

  Obtaining an LC is a common way of ensuring payment in international transactions. However, your foreign buyer may provide you with an LC or other banking instrument that has been issued by a fake bank, or is printed on the letterhead of a reputable international bank but was not actually issued by that bank (it is a forgery, in other words). The upshot is that you don't get paid.

  To eliminate the possibility of receiving a fraudulent LC, you should always have a bank confirm that an LC from a foreign buyer was issued by a legitimate foreign bank. The bank that provides this service for you is called the *advising bank*, and its role is to ensure that all documents are genuine and meet the conditions set out in the LC. Canadian exporters most commonly use Canadian banks as advising banks.

- **Fraudulent cheques**

  A foreign cheque can take a long time to cash. Your bank may not realize that it was fraudulent until weeks or months after you deposited it to your account. By then, the goods you shipped will be long gone and your bank will reduce the cash in your account by the amount of the fake cheque. Again, you haven't been paid for your goods.

- **Fraudulent buyer credit references**

  To obtain credit terms, your buyer may manufacture credit references in collusion with other parties. By the time you realize you've been deceived and that your buyer's credit is no good, the buyer has the goods and you are never paid for them.

These are the tried and true methods of defrauding exporters. As time passes, unfortunately, criminal organizations will not only develop subtle variants of them but will also use new technology and economic and political changes to continue victimizing both exporters and importers.

IF YOU'RE AN IMPORTER

For importers, financial fraud is usually based on getting you to pay for substandard goods or goods that are never shipped. If you can arrange to pay after you accept delivery of the goods and after you inspect them, you are much less likely to be defrauded. Such terms of sale, however, may not be available to you since they are often reserved for large buyers.

[6] Canada's OSFI (the federal bank regulator) considers trade finance products to be a business line that presents higher risks for money laundering and terrorist financing. See Appendix B.

Using a reputable international inspection firm can help ensure that the goods you ordered are the goods you receive. Trade finance products such as LCs and documentary collections can also help mitigate this risk although, as indicated earlier, they themselves can be used for criminal purposes.

The following frauds are the ones most commonly perpetrated against importers:

PREPAYMENT TO THE FOREIGN SELLER

Some foreign companies will offer favourable pricing and payment terms if you agree to pay partially or in full before receiving their goods. Here, the financial fraud occurs because the foreign seller never delivers the promised merchandise.

For an example, let's return to the hapless CIRC Systems and its central European nemesis, Blackbeard Ltd. CIRC intends to buy some goods from Blackbeard and sends a purchase order to this effect. When Blackbeard receives the order, it informs CIRC that it will reduce the price of the goods by 25 per cent if the Canadian company pays in advance.

Not wanting to turn down an apparently excellent opportunity, CIRC wires the payment to Blackbeard and waits for confirmation that the shipment is underway. But the goods never arrive and CIRC suffers financial damage as a result.

Sadly, CIRC could have avoided this damage if it had decided to forego the discount and insisted on paying Blackbeard only on receipt of goods, possibly through an LC. In this case, Blackbeard would probably have cancelled the transaction, since it never intended to ship the goods anyway, and CIRC would have kept its money.

GOODS-RELATED FRAUD

If you're the importer, you can be victimized through the goods involved in the transaction, which may be of inferior quality or shipped in insufficient quantity.

- **Goods of inferior quality**

  In this example, CIRC Systems receives a shipment of goods from Blackbeard Ltd., which CIRC has paid for in advance. On inspecting the goods, CIRC discovers that they are not as originally represented by Blackbeard but are of inferior quality. The merchandise cannot even be considered a legitimate substitute for the intended goods, which was permissible under the original sales agreement. In this case, Blackbeard has committed a crime, since collecting payment and then substituting inferior goods for the proper merchandise constitutes fraud.

  CIRC has made two fundamental errors here: it paid in advance and it didn't carry out due diligence on Blackbeard to see if the foreign firm had a history of shipping shoddy goods. Even if Blackbeard didn't appear to have such a reputation, CIRC still should have thought twice about paying in advance. Payment on satisfactory inspection of goods would have been a much safer approach.

- **Insufficient quantity of goods**

  If the amount of goods you receive from the foreign seller is less than the contracted amount, the seller must either adjust the invoice or send the missing goods in a timely manner.

Suppose CIRC Systems has paid Blackbeard Ltd. in advance for a shipment of 1,000 widgets, but only receives 950 widgets. Despite numerous attempts to correct the situation, CIRC receives neither the remaining widgets nor a refund for them. In this case, Blackbeard has committed fraud by collecting payment and then failing to furnish the proper amount of goods without offering a suitable remedy.

As in the previous example, CIRC should not have paid in advance, but only on receipt of the goods in full. In this case, when the order was short 50 widgets, CIRC could have held back payment for the undelivered items.

METHODS USED IN GOODS-RELATED FRAUD

There are four main techniques used in goods-related fraud, all of which involve forgery or counterfeiting in one way or another.

- **Fraudulent inspection companies**

  The inspection company's letterhead, web site and voice at the end of the telephone line all seem legitimate. Unfortunately, the entire organization is a fraud. Given the ease of setting up such a fake, you must make *very, very* sure that the inspection company you use is a genuine, reputable one, *especially* if it was recommended by your foreign supplier. In fact, best practice in this area is that the inspector should be completely unrelated to the supplier, so it's much better to find your own than to accept a supplier's recommendation.

- **Fraudulent inspection certificates**

  The inspection certificate is a forgery, although its letterhead appears to be that of a legitimate inspection company. In this case, the inspection company has never seen, let alone examined, the goods you've received.

- **Counterfeit finished goods**

  The goods you receive are counterfeit – that is, they were not manufactured by the company that holds a legitimate licence to make them, but by some other firm. They are invariably of inferior quality and unlicensed.

- **Counterfeit components**

  To shave costs, your seller includes counterfeit components when assembling its products. This can lead to substandard performance or product failure. If this happens, you may face costly litigation from your customers.

WHAT YOU SHOULD DO

If you suspect that a transaction with a foreign counterparty may involve financial fraud, you should do the following:

- Retain legal counsel to advise you how to proceed.
- Gather all supporting documentation and place it in a secure location.
- Notify your local law enforcement that you suspect a transaction may be related to financial fraud.

CHAPTER 5: CORRUPTION

Canada's *Corruption of Foreign Public Officals Act* (CFPOA) applies to Canadian businesses trading abroad and is based on the principles of the United Nations Convention Against Corruption.[7]

A Canadian company that makes payments to foreign public officials to gain a market advantage is participating in bribery. This is considered a serious offense both here and in most other countries because it propagates corruption in national economies and rots them from within. The bribing company can be prosecuted in Canadian courts under the CFPOA and the financial penalties, if it is convicted, can far outweigh any gains from the bribe. A recent case investigated by the RCMP under the CFPOA produced a landmark ruling in Canadian legal history and resulted in a fine of C$9.5 million for the company involved. In addition, the CFPOA provides for prison terms of up to fourteen years for individuals convicted of bribery.

Given the complexity of the CFPOA, you should always obtain legal advice when trying to determine how or whether the legislation might apply to your company. For a list of possible defences against a charge under the CFPOA, see Appendix A.

COMMON BRIBERY SITUATIONS

The following two examples illustrate how a potential bribery situation, which would be subject to the provisions of the CFPOA, might come about.

BRIBERY BY THE CANADIAN EXPORTER

Suppose CIRC Systems is in the process of selling some goods to Blackbeard Ltd., a company in central Europe. Abruptly, Blackbeard informs CIRC that the Canadian company must make a payment to the personal bank account of the local Minister of Finance to ensure that the goods can be sold to local government agencies.

Without this payment, Blackbeard adds, CIRC is unlikely to make any of these sales and may also face sanctions from the Ministry of Finance in Blackbeard's country.

In this case, CIRC realizes it is being asked to a bribe a public official. It very wisely cancels the transaction and severs all ties with Blackbeard.

BRIBERY FOR RELEASE OF GOODS TO THE CANADIAN IMPORTER

The foreign supplier may tell you that you must make a payment to a public official before it can release the goods you wish to purchase, or have already purchased.

[7] For the preamble to this Convention, see Appendix B.

These payments may be presented as a way of gaining favourable treatment for your shipment.

Suppose CIRC Systems purchases goods from Blackbeard Ltd., with payment due when CIRC receives the shipment. At this point, Blackbeard announces that if CIRC pays a sum of money to the Minister of Finance, the goods can be shipped from Blackbeard's country to Canada without customs inspection or the levy of export duties. Without the payment, Blackbeard adds, it may be very difficult to get the goods released so they can be shipped to Canada. If CIRC agrees, it should pay a "consulting fee" to the bank account of Yellow Co., a Caribbean company owned by the Minister.

CIRC, however, is aware that this is a bribe by another name. The company immediately cancels the transaction and refuses to have anything else to do with Blackbeard.

EXTRATERRITORIALITY: THE UNITED STATES

In the United States, the Foreign Corrupt Practices Act (FCPA) applies to American trading companies and to foreign companies that engage in commercial transactions in which a segment of the transaction is undertaken within the United States.

Because most international trade involves U.S. dollars, using U.S. currency for a corruption-related payment (such as a bribe) will invoke the FCPA even if the foreign company has no presence within the United States. Since a payment in U.S. dollars will involve an American correspondent bank, a portion of the transaction will have occurred in the United States.

The FCPA's extraterritoriality provisions can compound any allegations of corruption against a Canadian firm, since the company may be prosecuted under the anti-corruption laws of both the United States and Canada. As with the CFPOA, you should obtain legal advice if you think the FCPA might be applied to you.

EXTRATERRITORIALITY: THE UNITED KINGDOM

In the United Kingdom, the *Bribery Act 2010* (the "Bribery Act") provides a legal framework for combating bribery both domestically and abroad. The Act creates the following offences:

- active bribery, which is promising or giving a financial or other advantage;
- passive bribery, which is agreeing to accept a financial or other advantage;
- bribery of foreign public officials; and
- the failure of a commercial organization to prevent bribery by a person associated with the organization.

BRIBERY AND AGENTS

When bribery rears its head in international trade, the bribes are often linked to agents. The role of agents in corruption was examined in more detail in **page 14**, "Agency risk."

Because the law is extraterritorial, people and companies can be prosecuted for the above crimes even if the bribery takes place outside the United Kingdom. It applies to U.K. citizens and residents, and to companies established under U.K. law. Non-U.K. companies can be held liable for a failure to prevent bribery if they do business in the U.K.

Companies can be liable for bribery committed for their benefit by their employees or by other associated persons, and can also be culpable for board-level complicity in bribery, including bribery through intermediaries. There is also personal liability for senior company officers who turn a blind eye to such board-level bribery.

Penalties are stringent, providing for unlimited fines and terms of imprisonment of up to 10 years. You should obtain legal advice if you think the Bribery Act might be applied to you.

CORRUPTION AND MONEY LAUNDERING

Because corrupt government officials must ensure that the proceeds of crime have been laundered before they can spend the money, there is a strong link between corruption and money laundering. Nations around the world understand this relationship and have embedded anti-money-laundering defences within their financial systems.

The FATF has put considerable effort into investigating the connection between money laundering and corruption. For more information, refer to its reference guide on corruption.

BRIBERY LEGISLATION: DIFFERENCES AND SIMILARITIES

Canadian and U.S. anti-bribery laws are broadly similar, making compliance somewhat easier for companies that operate in these two countries. U.K. laws are stricter in that they cover not only the bribery of foreign government officials but also corruption between commercial entities.

WHAT YOU SHOULD DO

You can minimize your risk of becoming involved in corruption by taking these steps:

- Determine whether your market presents a high risk of corruption.
- Familiarize all employees with the *Corruption of Foreign Public Officials Act*.
- Establish a corporate anti-corruption policy that documents and applies suitable management systems for combating bribery.
- Require your employees and agents to periodically sign an agreement stating that they will comply with your anti-corruption policy.
- Educate and train your employees and agents about their anti-corruption responsibilities and the actions they should take if they encounter corruption.
- Verify the credentials of agents and partners representing your company and monitor their efforts on your behalf.
- Establish a reporting system for suspicious behaviour.

EDC also has **numerous resources** that can help you avoid involvement in corruption.

If you suspect bribery and/or corruption in your dealings with a foreign counterparty, you should promptly contact the International Anti-Corruption Unit of the RCMP in either Calgary (403-699-2550) or Ottawa (613-993-6884).

APPENDIX A: THE *CORRUPTION OF FOREIGN PUBLIC OFFICIALS ACT*

Canada's *Corruption of Foreign Public Officials Act* (CFPOA) applies to Canadian businesses trading abroad. The Act is based on the principles of the United Nations Convention Against Corruption.

Canada's CFPOA provides that:

3. (1) Every person commits an offence who, in order to obtain or retain an advantage in the course of business, directly or indirectly gives, offers or agrees to give or offer a loan, reward, advantage or benefit of any kind to a foreign public official or to any person for the benefit of a foreign public official or conceal such activity in its books and records:

   a. as consideration for an act or omission by the official in connection with the performance of the official's duties or functions; or

   b. to induce the official to use his or her position to influence any acts or decisions of the foreign state or public international organization for which the official performs duties or functions.

APPENDIX B: **OFFICE OF THE SUPERINTENDENT OF FINANCIAL INSTITUTIONS GUIDELINE B-8**

In 2008, Canada's banking regulator – the Office of the Superintendent of Financial Institutions (OSFI) – published its Guideline B-8, *Deterring and Detecting Money Laundering and Terrorist Financing*.

The Guideline classifies trade finance[8] as a business line that presents specific higher risks for money laundering and terrorist financing. As a result, the OSFI has prescribed various measures to enhance due diligence and other controls related to these higher-risk areas. To quote the Guideline:[9]

- Where the assessed risk of (money laundering and terrorist financing) in trade finance services is elevated, (federally regulated financial institutions) should take reasonable measures designed to mitigate the risk of misuse of trade financing mechanisms. Reasonable measures could include:
  - Conducting periodic on-site assessment of the risks posed by clients and the procedures they follow.
  - Reviewing the routing of shipments and noting ports of call or transhipment points that are inconsistent with a standard commercial transaction. For example, a shipment of steel from Canada to Asia might be routed via a European port or a country where there is no apparent business rationale for the routing, or the routing or the carrier may be located in a high-risk country.
  - Subjecting requests involving LCs that are inconsistent with the applicant's normal business patterns to more detailed review and noting the results in the client's records.
  - Identifying significant differences (either among different clients, different shipments or different market quotes) in the prices of the goods being financed under an LC, and determining the business rationale for the differences.
  - Making additional enquiries about the business rationale of transactions involving multiple banks and payments flowing through intermediaries, as opposed to flowing directly from the importer's bank to the exporter's bank.

[8] "Trade finance" refers to trade-related products and services offered by financial institutions, such as LCs, documentary collections and other financial instruments.
[9] The quoted text has been slightly edited for clarity.

APPENDIX C: **THE UNITED NATIONS CONVENTION AGAINST CORRUPTION (PREAMBLE)**

The preamble to the United Nations Convention Against Corruption reads, in part, as follows:

- The States Parties to this Convention,

  Concerned about the seriousness of problems and threats posed by corruption to the stability and security of societies, undermining the institutions and values of democracy, ethical values and justice and jeopardizing sustainable development and the rule of law,

  Concerned also about the links between corruption and other forms of crime, in particular organized crime and economic crime, including money-laundering,

  Concerned further about cases of corruption that involve vast quantities of assets, which may constitute a substantial proportion of the resources of States, and that threaten the political stability and sustainable development of those States,

  Convinced that corruption is no longer a local matter but a transnational phenomenon that affects all societies and economies, making international co-operation to prevent and control it essential....

Have agreed as follows (that) the purposes of this Convention are:

(a) To promote and strengthen measures to prevent and combat corruption more efficiently and effectively;

(b) To promote, facilitate and support international cooperation and technical assistance in the prevention of and fight against corruption, including in asset recovery;

(c) To promote integrity, accountability and proper management of public affairs and public property.

Ce document est également disponible en français.