UNCITRAL UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

Recognizing and Preventing Commercial Fraud

Indicators of Commercial Fraud
Prepared by the UNCITRAL Secretariat

UNITED NATIONS

Further information may be obtained from:

UNCITRAL secretariat, Vienna International Centre,
P.O. Box 500, 1400 Vienna, Austria

Telephone: (+43-1) 26060-4060 Telefax: (+43-1) 26060-5813
Internet: www.uncitral.org E-mail: uncitral@uncitral.org

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

Recognizing and Preventing Commercial Fraud

Indicators of Commercial Fraud
Prepared by the UNCITRAL Secretariat

UNITED NATIONS
New York, 2013

This publication has not been formally edited.

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Contents

Introduction

A. Purpose and target audience

As early as 2002, the United Nations Commission on International Trade Law (UNCITRAL) first considered the problem of fraudulent practices that resulted in a significant adverse economic impact on world commerce and negatively affected legitimate commercial institutions. Through a series of consultations with experts and government officials who regularly encountered and combated commercial fraud and who represented different regions, perspectives, and disciplines, UNCITRAL became aware of the widespread existence of commercial fraud and its significant worldwide impact, regardless of a country's level of economic development or system of government. In considering possible responses to this threat, it was felt that education and training could play significant roles in fraud prevention, and that the identification of common warning signs and indicators of commercial fraud could be particularly useful in combating fraud.

To this end, the UNCITRAL Secretariat met over the ensuing years with international experts and government officials knowledgeable in the identification and prevention of commercial fraud, and as a result developed the attached list of twenty-three indicators of commercial fraud. The overall objective of this project was to assist in the prevention of commercial fraud by creating an easily understood and widely-disseminated document that set out indicators to assist potential victims and their organizations in the identification of behaviour that could be associated with or could constitute commercial fraud. Governments and other bodies and organizations are encouraged to disseminate these materials as widely as possible, and to encourage their use in the prevention of fraud.

It is hoped that, in addition to preventing the perpetration of specific commercial frauds through education and awareness, this anti-fraud project will serve three main overarching purposes. First, these materials are intended to identify patterns and characteristics of commercial fraud in a manner that facilitates the private sector in combating commercial fraud in an organized and systematic manner. Second, it is hoped that governmental bodies may be assisted by these materials in understanding how to help the public and private sectors to address the problem of commercial fraud. Finally, these materials may assist the criminal law sector in understanding how best to engage the private sector in the battle against commercial fraud.

These materials are not intended as a legislative text nor a legal text, but rather as instructive materials containing useful guidance and reference materials for users. It is hoped that financial decision-makers and those charged with combating commercial fraud can learn and benefit from these materials, be they individual investors or purchasers, CEOs, bank executives, law enforcement agencies or regulators, or the board of directors of any company, large or small. Even decision makers charged with distributing emergency relief or crisis funds on behalf of governments or international organizations may benefit from recognizing and remaining alert to these potential indicators of fraud. In addition, third parties such as employees of banks or other entities, or professionals assisting in a transaction or an investment, must be aware that they may unwittingly assist in the perpetration of a fraud by simply being blind to the indicators of a potential fraud.

Examination of the various indicators has revealed that they tend to be present in many different cases of potential fraud, regardless of the level of sophistication of the financial decision maker, or of the development of a particular economy involved. In an effort to illustrate this point, the instances and examples that are given in these materials for each of the indicators are drawn from various different areas of legal practice and include different types of victims. They are intended to demonstrate that the indicators are meant to be of universal application in a commercial and administrative context; the only quality that the victims are certain to share is a vulnerability to fraud that stems from their role as a financial decision maker.

However, it is important to remember that each of the indicators taken alone or in combination is not intended to definitively indicate the presence of commercial fraud. Instead, the presence of a single warning sign is intended to send a signal that commercial fraud is a possibility, while the presence of several of the indicators should heighten that concern.

The presentation of each of the indicators is similar: first, the indicator is identified, followed by a more detailed description of the indicator, which is in turn followed by instances and examples of the particular indicator as found in a commercial fraud in a variety of different contexts. Advice is then provided regarding what may be done to avoid or to counteract the effects of the behaviour identified in each indicator, as appropriate. Finally, many of the indicators may and should overlap, since identification of them is not an exact science, and these materials include cross references to related indicators, where relevant.

B. History

At its thirty-fifth session in 2002, UNCITRAL first considered whether the problem of fraudulent practices of an international character resulted in a significant adverse economic impact on world commerce and negatively affected legitimate commercial institutions. It was felt that fraudulent practices that affected international commerce had not been sufficiently addressed by international bodies, particularly with respect to their commercial aspects. It was suggested that UNCITRAL was well-positioned to consider the issue of commercial fraud, since it presented the unique combination of a governmental perspective with recognized expertise in international commerce and a tradition of collaboration with other international organizations.[1]

In order to assess the extent and implications of commercial fraud and to consider possible recommendations regarding future action, in December 2002, the UNCITRAL Secretariat convened a meeting of experts who regularly encounter and combat commercial fraud and who represented different regions, perspectives, and disciplines. Following that meeting, the UNCITRAL Secretariat prepared and issued a note on possible future work relating to commercial fraud (A/CN.9/540) as requested by UNCITRAL at its thirty-fifth session. The note concluded that available evidence suggested that commercial fraud constituted a serious and potentially increasing threat to international commerce. The note also considered factors in defining or describing commercial fraud, concluding that a precise definition was not currently available but that it would be useful to identify and detail common patterns of fraudulent commercial conduct. Finally, the note also suggested that there was an important independent commercial dimension to commercial fraud in addition to that of criminal law enforcement, and made several recommendations to UNCITRAL in regard to future work.

At its thirty-sixth session in 2003, UNCITRAL considered the note of the Secretariat (A/CN.9/540). It agreed with the recommendation that an international colloquium should be organized to permit an exchange of views from various interested parties, including those working in national Governments, intergovernmental organizations and relevant private organizations on the private law aspects of commercial fraud. It was also noted that the colloquium would provide an opportunity to promote an exchange of views with the criminal law and regulatory sectors that combat commercial fraud and to identify matters that could be coordinated or harmonized.[2]

A colloquium on international commercial fraud was held in Vienna from 14 to 16 April 2004. The speakers, panellists and participants at the colloquium consisted of experts from each of several legal practice areas examined, representing as broad a spectrum of approaches to the problem of commercial fraud as possible, and included approximately 120 participants from 30 countries. It was agreed at the colloquium that any doubt had been dispelled as to the widespread

[1] *Official Records of the General Assembly, Fifty-seventh Session, Supplement No. 17* and corrigendum (A/57/17 and Corr.3), paras. 279-290.

[2] Ibid., *Fifty-eighth Session, Supplement No. 17* (A/58/17), paras. 240-241.

existence of commercial fraud and its significant worldwide impact, regardless of a country's economic development or system of government. It was also agreed that education and training played significant roles in fraud prevention and that it would be particularly useful to identify common warning signs and indicators of commercial fraud. In addition, it was agreed at the colloquium that local cooperative efforts between law enforcement bodies and the private sector seemed particularly effective and should be encouraged (see A/CN.9/555, paras. 3, 4, 25-28, and 62-71).

At its thirty-seventh session in 2004, UNCITRAL considered the report of the UNCITRAL Secretariat on the colloquium (A/CN.9/555), and, inter alia, agreed that, with a view towards education, training and prevention, the preparation of materials setting out common features present in typical fraudulent schemes could be useful as educational material for participants in international trade and other potential targets of perpetrators of fraud. It was thought that such materials would help potential targets protect themselves and avoid becoming victims of fraudulent schemes. Further, it was thought that national and international organizations interested in fighting commercial fraud could be invited to circulate such material among their members in order to help test and improve those lists. While it was not proposed that UNCITRAL itself or its intergovernmental working groups be directly involved in that activity, it was agreed that the UNCITRAL Secretariat should consider preparing, in close consultation with experts, such materials listing common features present in typical fraudulent schemes.[3]

At its thirty-eighth session in 2005, UNCITRAL reiterated its support for this project,[4] and at its thirty-ninth session in 2006, UNCITRAL further approved of the general approach taken in the drafting of these materials as set out in a note by the Secretariat (A/CN.9/600).[5] At its fortieth session in 2007, UNCITRAL reviewed the results of that work as reflected in a note by the Secretariat entitled "Indicators of commercial fraud" (A/CN.9/624 and Add.1 and 2), commended the work accomplished and agreed that the indicators should be circulated for comment.[6] Finally, at its forty-second session in 2008, UNCITRAL considered the comments of States and organizations on the indicators that had been submitted to the Secretariat (A/CN.9/659 and Add.1 and 2) and decided to publish the materials as a Secretariat informational note for educational purposes and fraud prevention.[7] This text was most recently updated in 2013.

For further information, please visit the UNCITRAL website at www.uncitral.org.

[3] Ibid., *Fifty-ninth Session, Supplement No. 17* (A/59/17), paras. 110-112.

[4] Ibid., *Sixtieth Session, Supplement No. 17* (A/60/17), para. 220.

[5] Ibid., *Sixty-first Session, Supplement No. 17* (A/61/17), para. 217.

[6] Ibid., *Sixty-second Session, Supplement No. 17* (A/62/17), paras. 199-200.

[7] Ibid., *Sixty-third Session, Supplement No. 17* (A/63/17), paras. 342-343.

C. What is commercial fraud?

It would not be appropriate to set out a strictly legal definition of commercial fraud in light of the aims and objectives of these materials, nor would such a definition allow sufficient flexibility for the intended broad use of these materials. However, a descriptive definition outlining the main elements of commercial fraud could be helpful to the user of these materials.

The following elements are key to the identification of commercial fraud:

(1) There is an element of deceit or of providing inaccurate, incomplete or misleading information;

(2) Reliance on the deceit or the information provided or omitted induces the target of the fraud to part with some valuable thing that belongs to the target or to surrender a legal right;

(3) There is a serious economic dimension and scale to the fraud;

(4) The fraud uses or misuses and compromises or distorts commercial systems and their legitimate instruments, potentially creating an international impact; and

(5) There is a resultant loss of value.

Further, the term "fraudster" has been used in these materials as a term to identify someone who is perpetrating, or attempting to perpetrate a fraud.

D. Related topics

A number of serious issues related to commercial fraud have not been covered in these materials in order to keep them of a manageable and useful size, and since such issues have been, and are continuing to be, dealt with in other forums or by other organizations. A non-exhaustive list of such issues, and some suggestions regarding where further information can be found, appears below. Note also that the suggested sources for further information are limited to international organizations, and that there are numerous national governmental and non-governmental organizations which have also worked extensively in these areas, and to which resort should be had for more information. All websites noted were last visited on 1 July 2013.

1. Corruption and bribery

Corruption has been defined by Transparency International as "the abuse of entrusted power for private gain". Further differentiation has been made between "according to the rule corruption" and "against the rule corruption", wherein the former includes facilitation payments, where a bribe is paid to receive preferential treatment for something that the receiver of the bribe is required to do by law, while the latter includes bribes to obtain services that the receiver of the bribe is prohibited from providing.

A number of international organizations have adopted instruments, including conventions, aimed at fighting corruption and bribery. These organizations include: the United Nations; the African Union; the Council of Europe; the European Union; the Economic Community of West African States; the Organization of American States; and the Organisation for Economic Co-operation and Development.

There is a large amount of information available concerning corruption and bribery, including materials on how to combat it. The following lists a few of the many sources of such information:

- Transparency International; www.transparency.org
- United Nations Office on Drugs and Crime; www.unodc.org/unodc/en/corruption/index.html?ref=menuside
- Organisation for Economic Co-operation and Development; www.oecd.org/corruption
- Organization of American States; www.oas.org/juridico/english/FightCur.html
- The World Bank; www.worldbank.org/anticorruption
- APEC Anti-Corruption and Transparency Working Group; http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Anti-Corruption-and-Transparency.aspx
- Financial Action Task Force; www.fatf-gafi.org/topics/corruption
- INTERPOL; http://www.interpol.int/Crime-areas/Corruption/Corruption

2. Money-laundering

Money-laundering may be described as the practice of engaging in specific financial transactions in order to conceal the identity, course, and/or the destination of money. A number of national and international rules and programmes have been developed to combat money-laundering.

Again, there is a great deal of information available on money-laundering, both nationally and internationally. For example, resort may be had to:

- United Nations Office on Drugs and Crime; www.unodc.org/unodc/en/money-laundering/index.html?ref=menuside
- Financial Action Task Force; www.fatf-gafi.org/topics/corruption
- International Bar Association Anti-Money-Laundering Forum; www.anti-moneylaundering.org
- INTERPOL; www.interpol.int/Crime-areas/Financial-crime/Money-laundering

3. Transparency

"Transparency" has been defined, again by Transparency International, as "a principle that allows those affected by administrative decisions, business transactions or charitable work to know not only the basic facts and figures, but also the mechanisms and processes" by means of which the decisions were made and transactions entered into. It is further said that "it is the duty of civil servants, managers and trustees to act visibly, predictably and understandably".

As a general principle, true transparency should be sought in all transactions and if achieved, should result in the prevention and avoidance of commercial fraud.

For further information, sources that may be consulted are:

- Transparency International; www.transparency.org
- World Bank; www.worldbank.org
- APEC Anti-Corruption and Transparency Working Group; http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Anti-Corruption-and-Transparency.aspx
- European Union Transparency Register; http://europa.eu/transparency-register/

4. Best practices

"Best practices" are, in this case, those techniques, methods, processes, activities or the like, used by highly respected organizations, public and private, that are focused on the prevention or detection of commercial fraud, and that should be adopted by entities such as companies and financial institutions and consistently followed by their employees. If such approaches are followed, and the proper processes, checks and testing have taken place, those systems should assist greatly in the prevention or detection of a fraud. Entities and organizations should be sure to investigate and adopt the best practices most suited to their operations, and should investigate them by way of their professional organizations or consult with private sector specialists.

(1) Corporate governance

The term "corporate governance" is the set of processes, laws, policies and institutions affecting the way a corporation is directed, administered and controlled, and involves the set of relationships between the company's management, its board of directors, its shareholders and other stakeholders. At the core of corporate governance are issues such as corporate fairness, transparency, fiduciary duty and accountability.

Establishing and adhering to the principles of good corporate governance should assist greatly in the prevention of commercial fraud either on the company, or on other parties, with the assistance of employees.

A great deal of material has been published on this topic, and resort could be had to the following sources:

- Organisation for Economic Co-operation and Development; www.oecd.org/corporate

- The European Corporate Governance Institute; www.ecgi.org

- International Finance Corporation (World Bank Group); http://www.ifc.org/wps/wcm/connect/Topics_Ext_Content/IFC_External_Corporate_Site/Corporate+Governance

(2) Whistle-blower policies

A "whistle-blower" is someone, usually an insider, who reveals wrongdoing within an organization to the public or to those in positions of authority. Whistle-blowing policies operate to give adequate protection to those who wish to come forward to report deviations from legal or ethical corporate standards. This can be done, for example, via confidential telephone services or intranet sites through which employees and business partners can address concerns or pass information. To make such services effective, genuine concerns must be listened to and acted upon in a timely manner by the responsible board committee.

The adoption of adequate whistle-blower policies by an organization, and education of employees about the existence and anonymity of such processes, can aid greatly in the detection of fraud or wrongdoing within an organization.

Again, much has been written on this topic, for example by:

- Transparency International; www.transparency.org

(3) Role of internal and external auditors

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. Internal auditors are employees of the entity who report to a general or chief auditor, who, in turn, reports to the Audit Committee of the Board of Directors.

An external auditor consists of audit professionals who perform an audit on the financial statements of a company, individual or other organization, its key characteristic being that it is independent from the entity being audited. The external auditor also reports to the Board of Directors of an organization, and may also be required by specific legislation to make submissions to regulatory agencies.

Both types of audits are useful and recommended to detect fraudulent activity and to assist in its prevention.

Again, reference may be had to:

- Transparency International; www.transparency.org

- Organisation for Economic Co-operation and Development; www.oecd.org

I. Indicators of commercial fraud

Indicator 1. Irregular documents

Indicator 2. Misuse of technical terms

Indicator 3. Inconsistencies in the transaction

Indicator 4. Misuse of names

Indicator 5. Disproportionate returns

Indicator 6. Undue secrecy

Indicator 7. Overly complex or overly simplistic transactions

Indicator 8. Frustration of due diligence

Indicator 9. Abuse of incentives

Indicator 10. Psychological inducements and ensnarement

Indicator 11. Crisis-caused breakdowns in preventive controls

Indicator 12. Immediate, fast or irrevocable transfer of funds

Indicator 13. Questionable or unknown source of repayment

Indicator 14. Irrational or illogical aspects or explanations

Indicator 15. Fraud based on abuse of personal affinity or relationships

Indicator 16. Fraud by or involving employees

Indicator 17. Unusual involvement or participation of professionals

Indicator 18. Inappropriate requests for information disclosure

Indicator 19. Misuse of technology and electronic fraud

Indicator 20. Pyramid and multi-level marketing schemes

Indicator 21. Frauds involving goods and services

Indicator 22. Securities fraud and market abuse

Indicator 23. Misuse of insolvency proceedings

Indicator 1. Irregular documents*

1. Commercial frauds almost always involve the issuance of, use of, or reliance on documents that are not normally or typically used in the type of transaction to which they are intended to relate, or on documents that contain discernible irregularities either individually, or when read in light of all the documents presented in support of the scheme.

A. Explanation

2. Commercial frauds, like legitimate transactions, involve the use of multiple documents to explain, memorialize and reflect the transaction. However, the documents used in commercial frauds often differ from those used in legitimate transactions either because they are improperly drafted, or because they contain some unusual features to induce investment, to bolster the fraudster's credibility, to explain the extraordinary returns claimed by the fraudster, or they set out unusual procedures. It is often possible to determine the likelihood or presence of a commercial fraud by identifying these irregular aspects. Documents used in support of a commercial fraud can be genuine, fraudulent, forged or fictitious, and can be issued or authenticated either properly or improperly by institutions or individuals. Sometimes professionals can be involved in their creation or authentication.

B. Instances and examples

3. Documents that may be used in connection with commercial frauds include:

(a) Genuine documents;

Illustration 1-1: Such documents may include: studies by organizations; letters of introduction; written attestations that an individual has an account in the institution or is a customer of the institution; a contract drafted by a lawyer; an authenticated telecommunication or funds transfer or SWIFT.

(b) Fictitious documents that are not used in legitimate commerce;

Illustration 1-2: Such documents may include: an "irrevocable SWIFT"; "UCP500 Forfait Transaction" or "Grain Warrants".

(c) Forged or fraudulent documents;

Illustration 1-3: An employee forges the signature of a bank manager on a letter provided by the fraudster.

*Note that throughout these materials, references to 'documents' are intended to include references to electronic communication and records.

Illustration 1-4: Documents that are commonly forged or fraudulent may include a forged signature or misdescription of goods on a bill of lading; a bank guarantee; documents under a commercial letter of credit; or false audit reports.

(d) Counterfeits of genuine documents.

Illustration 1-5: Documents that are commonly counterfeited include stock certificates; debentures; promissory notes; precious metal depositary certificates; warehouse certificates; or government procurement contracts, all of which may be used to induce investment in a fraudulent investment scheme or hypothecated to obtain an extension of credit from a legitimate financial institution.

4. Legitimate institutions or their employees can be knowingly or unwittingly induced to issue or verify legitimate or illegitimate documents that are then used to enhance the fraudulent scheme. Electronic verification may also be requested.

Illustration 1-6: A clerk is asked to issue or authenticate a document that is not usually issued by that clerk or by that institution. Or, the requester of the document seeks the inclusion of unusual phrases such as that funds are of “non-criminal origin”, or may request the insertion of legitimate commercial terms such as that the customer is “ready, willing, and able” to enter into transaction. The clerk obliges in order to assist the customer but without understanding the document or phrases, and the documents are subsequently used to bolster the credibility of the fraud.

Illustration 1-7: A clerk authenticates a document prepared by a customer on bank or company stationery. Although the clerk intends only to authenticate the signature or identity of the customer, the document contains statements that are used to enhance credibility by indicating that the bank or company attests to what is said in the document.

5. The irregularities in documents used in commercial fraud may be caused by or connected with professionals.

Illustration 1-8: A lawyer, accountant or other professional prepares documents at the request of a client regarding a transaction that the professional does not inquire into or does not understand, and that does not make economic or other sense. The fraudster often needs the professional to give credibility to his or her scheme. Agreeing to witness or confirm a pre-signed document would be a particular example of a transaction that could facilitate a fraud.

6. A commercial fraud may be signalled by:

(a) An absence of proper documentation;

Illustration 1-9: The existence of only a few poorly drafted documents for a major transaction; or a bank loan without a business plan to repay money.

(b) Documents that are issued by a genuine commercial entity but contain irregularities in connection with their issuance;

Illustration 1-10: A shipping clerk is asked to sign and postdate a document stating that goods, which have not yet arrived, have been received on the basis of the presenter's representation that goods will be received by that date. The presenter then uses the document to obtain payment, although goods are never delivered.

Illustration 1-11: A seller of real or personal property is asked to adjust the stated purchase price for real or personal property so that the buyer may increase the amount able to be borrowed or to decrease tax liability for the transaction or the property.

(c) Internal irregularities and inconsistencies in the documents;

Illustration 1-12: A document relating to a sophisticated transaction or one for a large sum contains spelling errors or grammatical errors, or has unprofessional-looking graphics or an unsophisticated appearance.

Illustration 1-13: Odd phrases or terms found in genuine documents, including: "NC/ND"; a document that is not a letter of credit is said to be subject to UCP500; performance in a "year and a day" or "a month and a day"; reference to "international banking seconds, hours or days".

Illustration 1-14: A transaction for a large amount of money that is disproportionate with the situation or the person with which it is connected, such as a small bank with assets of UK £75 million issuing a document for UK £100 million.

(d) The presence of a document that does not itself make sense or that does not make sense in connection with other documents involved in the transaction;

Illustration 1-15: In a transaction allegedly involving the sale of independent guarantees, a document was presented relating to factoring.

(e) The presence of incorrect or unusual headings of or in documents;

Illustration 1-16: What is supposed to be a letter of credit is entitled "Hypothecation Agreement" and contains a promise to pay funds to bearer.

(f) Documents that do not appear in the normal course of business;

(g) The unusual appearance or texture of a financial instrument;

Illustration 1-17: Document contains blurred typography, poor paper quality, spelling mistakes or an unprofessional look or graphics.

(h) The antedating or postdating of documents;

Illustration 1-18: A bill of lading stating that the goods are loaded on board a vessel is issued with a date a week earlier than the date the goods are said to have been loaded.

(i) Or changes in the existing documentation that fundamentally and inexplicably change the nature of the transaction.

Illustration 1-19: The transaction is said to relate to trading in sugar and, purportedly as a result of a difficulty, the documents are suddenly switched to relate to a sale of steel.

Illustration 1-20: The documentation was an independent guarantee and suddenly a promissory note.

C. Advice

7. Complete documentation of the investment should be required in advance and any unusual characteristics or aspects that are not understood in the form, content or authenticity of the documents should be investigated, especially where the investment involves financial instruments.

8. Read carefully documents presented in support of an investment and remember that they should be consistent in terms of the transaction as a whole.

9. Documents should not be antedated or postdated, and the dates referred to in them should be consistent.

10. Documents presented in support of a proposed commercial transaction should not be relied upon without considering their content, purpose and source.

11. Inquire whether the document is of a type that is regularly issued.

12. A general addressee, such as "To whom it may concern" should be cause for further inquiry.

13. Do not assume the authenticity of letterheads of well-known companies or organizations that could have been produced by laser printer.

14. Verify signatures.

15. Determine that professionals employed have an understanding of the documents they are preparing or verifying.

16. Perform thorough due diligence by consulting independent sources of information, or by consulting legal and risk management or security departments regarding the documents and their contents.

17. If critical reliance in a transaction is placed on a particular document, it should be produced.

18. Extreme caution should be exercised if engaging in a transaction where irregular or incomplete documents are used or relied upon as a matter of course in the trade.

19. Never grant power of attorney to persons unknown.

20. Do not sign, issue or authenticate documents that are unusual, that are not understood, that are not usually signed by the individual or institution being requested to sign them, or whose purpose is not understood.

21. Do not sign a document that is incomplete or that is in another language that is not understood.

22. Never sign or issue a statement that is known or suspected to be untrue.

23. Investigate whether the person requesting the service is a regular customer.

24. It may be advisable to set out the purpose for which the document was prepared in the body of the document itself, as a means to possibly avoid later misuse.

25. Be cautious of issuing unusual documents, particularly when the text is provided by the requester.

26. Use forms that are approved by legal and risk management or security departments.

27. If presented with a financial instrument that is unfamiliar in the marketplace, such as a stock certificate traded on a foreign exchange, have the document examined by a reputable expert in the field, like a stockbroker of good reputation.

D. Additional references

Indicator 3. Inconsistencies in the transaction; Indicator 4. Misuse of names; Indicator 6. Undue secrecy; Indicator 8. Frustration of due diligence; and Indicator 17. Unusual involvement or participation of professionals; Addendum 1. Performing due diligence.

Indicator 2. Misuse of technical terms

1. Commercial frauds misuse technical terms by using an actual term in an incorrect context or inventing an impressive sounding term to gain credibility, to obscure implausible aspects of the scheme, or to impress or intimidate victims or their advisors.

A. Explanation

2. Modern commerce and finance are complex and regularly use specialized terms related to a transaction or its financing. Commercial frauds frequently employ such terms to give the impression that the scheme is genuine, to impress or intimidate victims, or to cover their inability to explain inconsistencies or illegal aspects of the transaction. Since the fraudsters are often not knowledgeable themselves, they frequently misuse specialized terms, thereby signalling that the transaction is not genuine. Legitimate transactions occasionally may contain mistakes that are not essential to the transaction, and where a misuse is infrequent or the mistake is peripheral to the nature of the scheme, it is less likely to indicate commercial fraud. However, where the misuse is of a term essential to the scheme, and where it is consistent and frequent, it may indicate that the transaction is not legitimate.

B. Instances and examples

3. Technical terms can be misused to:

(a) Impress or overwhelm the victim;

Illustration 2-1: Fraudster gives a detailed but distorted discussion of macroeconomic history oriented towards reinforcing the credibility of the investment.

Illustration 2-2: Fraudster makes reference to major international agreements or programmes such as the Bretton Woods Agreements or the Marshall Plan to explain the overall scheme.

(b) Justify the inexplicable by resort to technical terminology;

Illustration 2-3: Funds in an account are said not to be at risk because they will be "scanned" by the trading bank, but not otherwise affected.

(c) Excuse a failure in promised performance;

Illustration 2-4: Government regulations, such as tax laws, or electronic funds transfer systems rules are referred to in explaining why the "trades" or payment is delayed, or why additional funds are required by the fraudster.

(d) Or build excessive reliance by the victim on the fraudster's apparently superior knowledge.

Illustration 2-5: Fraudster rationalizes the disproportionate returns of the scheme based on an economic analysis that explains how banks purportedly increase the money supply.

4. Misused technical terms may either exist and be used properly, may be used incorrectly or in an improper context, or may be entirely fictional.

Illustration 2-6: Actual terms such as "Factoring" or "Forfait" may be used incorrectly.

Illustration 2-7: Investment is said to involve trading in independent guarantees that do exist but are not "traded".

Illustration 2-8: Investment is said to be made on a specific form, such as "ICC Form 1020" or "SWIFT MT760", but the form does not exist or has a different purpose.

Illustration 2-9: Fraudster misuses or twists legitimate technical or scientific terms, such as a successful fraud in the oil and gas industry that referred to the fictional process of "sonic" fracturing (or "sonic fracking") to assist oil or gas recovery.

5. Technical terms may also be misused in different ways:

(a) At different stages of the scheme;

Illustration 2-10: For example, they may be used to entice the investor, to obtain funds, to induce the transfer of control of assets, to explain why payments are delayed, or to prevent the investor from contacting authorities.

(b) Or beyond their intended purpose in order to validate a transaction.

Illustration 2-11: Commercial frauds often use technical terms regarding funds transfer to purportedly indicate the legitimacy of the transaction, but which are in fact only intended to indicate that a particular message was sent, but do not authenticate its contents.

C. Advice

6. Do not be intimidated or impressed by the use of technical terms and jargon.

7. Insist on a clear explanation, regardless of the level of one's own knowledge or expertise.

8. Understand all aspects of the transaction before investing.

9. When performing due diligence, do not simply be satisfied with the existence of a specific technical term, such as "stand-by letters of credit", but ascertain whether the technical term or its role in the transaction is used properly in the context.

10. Check into the existence and operation of any law under which taxes, fees and other sums are allegedly owed.

11. Employees should be educated about commonly misused terms and phrases.

12. The appropriate employee within an organization should be consulted on a specialized transaction, or should be part of the negotiating or document review team.

D. Additional references

Indicator 6. Undue secrecy; Indicator 8. Frustration of due diligence; Addendum 1. Performing due diligence.

Indicator 3. Inconsistencies in the transaction

1. In attempting to mimic aspects of genuine transactions, commercial frauds often contain untrue or conflicting statements of material facts, omissions of material facts and other serious inconsistencies.

A. Explanation

2. Commercial transactions operate under rule-based systems; multiple aspects, documents, details and representations are consistent with one another and, taken as a whole, reflect the scope and purpose of the transaction. Any inconsistency or repeated inconsistencies that do not result from an agreed change in the transaction are removed in the case of legitimate commercial transactions. Transaction participants understand the representations and details and ensure that all aspects of the entire context of the transaction are consistent. On this basis, they may be confident in accepting transactional and contractual obligations.

3. In a sophisticated fraud, inconsistencies may not be obvious, such as in the case of frauds where professionals within seemingly reputable firms of lawyers, accountants and bankers may have been successfully misled by a fraudster, and have unwittingly assisted in creating fraudulent documentation. However, in a typical scheme, fraudsters are unlikely to concern themselves with transactional realities in their quest to find a potential victim. In fact, fraudsters may create inconsistencies intentionally, with the expectation that the more informed persons will walk away, leaving only those potential victims who are most vulnerable. Further, fraudsters are not necessarily concerned that all aspects of the context of the transaction be consistent. They often use old, pattern frauds, developed by others decades ago, and simply adapt these old schemes to the Internet, or replace old names with invented modern sounding fictitious instruments, such as "Anti-Terrorism/Drug Free Certificates" and may not know of the fraud's internal inconsistencies. Fraudsters often are not experts in the fields of investment or business contemplated by their frauds and, lacking such expertise, they inadvertently may create inconsistencies in the transaction within individual documents or between documents, or there may be inconsistencies between what is written and what is said on various occasions.

B. Instances and examples

4. The nature of the goods changes depending on the document examined.

> *Illustration 3-1:* At the outset, a transaction involves shipments of one commodity, but without any commercial explanation, the goods being sold are described as a different commodity in later documentation.

5. What is written or said is devoid of logic or common sense.

> *Illustration 3-2:* The goods described in the transaction, or a financial instrument described in the transaction, do not exist or are not commercially traded.
>
> *Illustration 3-3:* An invoice reflects ocean carriage, but the transport document reflects rail or truck transport only.
>
> *Illustration 3-4:* The first document refers to "ABC Corp" while later documents refer to "XYZ Corp", or one company may guarantee the first document, while another guarantees the second document.
>
> *Illustration 3-5:* Container or seal numbers listed on bills of lading or other transport documents are suspicious, or do not reflect the proper numbering and lettering systems.

6. Individual orders are out of context with the overall transactional history.

> *Illustration 3-6:* An unusual quantity of the same product is ordered with a demand for next-day delivery to be shipped to a mail-drop address.

C. Advice

7. Read documents critically, take detailed notes of any oral representations, and require any oral representations to be incorporated into the documents.

8. Do not rely solely on the documents presented for due diligence.

9. Ask questions about inconsistencies and do not accept facile answers or excuses. Suspicious or illogical explanations when inconsistencies are raised may signal fraud.

10. The presence of inconsistencies is unusual; the unresolved presence of inconsistencies is highly unusual; and both may signal fraud.

11. If a transaction or activity occurs that does not pass one's own "common sense" test, then that alone is a good enough basis to consider the matter suspicious and to pursue due diligence.

D. Additional references

Indicator 1. Irregular documents; Indicator 8. Frustration of due diligence; Indicator 14. Irrational or illogical aspects or explanations; Indicator 21. Frauds involving goods and services; Addendum 1. Performing due diligence.

Indicator 4. Misuse of names

1. The person promoting a fraudulent scheme often seeks to enhance personal credibility or that of the scheme by associating it with the names of persons or organizations known, or likely to be known, by the person or entity to which the scheme is presented.

A. Explanation

2. Names, particularly of those who are reputable or influential in the field, are misused in several ways in commercial frauds. Similarly, the names, logos, trademarks, catch-phrases and symbols of a company or other entity, can be used in the perpetration of a fraud. A fraudster may suggest that individuals known within the field have reviewed and approved of the purported transaction, thus suggesting to the victim credibility, validity and enforceability of the fraudulent scheme. A fraudster may introduce or promote a scheme by asserting a false or exaggerated relationship with a person or entity known to the victim or its advisors. A fraudster may give the name of a well-known person or entity as his or her own or suggest an association with it, or a fraudster may simply adopt the name of another person or entity to hide the fraudster's own identity.

B. Instances and examples

3. The names used in connection with commercial fraud may be of:

(a) Well-known persons or organizations;

Illustration 4-1: A fraudster claims to be a protégé of the head of a country's Central Bank or Ministry or similar body, who is alleged to have provided advice regarding the scheme, but whose role and/or identity is not revealed.

Illustration 4-2: The fraudster introduces the potential victim to an actual or purported relative of an eminent person, such as the prime minister or a president of a country, who is willing to vouch for the fraudster or his or her proposed transaction.

(b) Individuals with whom the potential victim or the victim's advisors are familiar;

Illustration 4-3: The fraudster claims that the potential victim's business partner or friend has participated in the transaction when, in fact, that person has not.

(c) Or well-known organizations and rules.

Illustration 4-4: Documentation provided by the fraudster mentions the United Nations, or the International Monetary Fund or the International Chamber of Commerce, but gives no explanation as to its relationship to the transaction. Other references may be to ICC Rules, UCP 500, or SWIFT when the nature of the transaction does not correspond with the rules cited, or, more generally, to the involvement or approval of other "federal" or "national" or international banking or other authorities.

4. A commercial fraud may be signalled where:

(a) The promoter of the transaction gives instructions concerning individuals or entities that the potential victim may wish to contact to verify the authenticity of the transaction:

Illustration 4-5: The fraudster suggests that an international or governmental entity approves of transactions of the type promoted. However, the fraudster warns the potential victim that if he or she contacts that body to ask about the transaction, the entity will be forced to deny the legitimacy of the transaction.

Illustration 4-6: The fraudster suggests that the president of a major bank has approved of the fraudster's transaction and suggests that the potential victim contact the president to discuss the transaction, even providing the president's telephone number and e-mail address. However, the potential victim's inquiries are in fact answered by the fraudster or a co-conspirator, who assures the potential victim of the legitimacy of the transaction.

(b) The potential victim cannot verify that the references made by the fraudster actually support the transaction:

Illustration 4-7: The fraudster states that a well-known celebrity or sports figure has invested in the fraudster's purported transaction. Because the victim cannot contact the celebrity directly to discuss financial transactions, the reference cannot be verified.

(c) Or telephone numbers given to verify information are mobile telephone numbers, or do not correspond geographically with the address given.

C. Advice

5. An independent investigation of claims of affiliation should be conducted. Most well-known organizations have public information against which claims

and documents can be compared for substantiation. However, note that elaborate schemes may involve the creation of false websites that mirror the authentic website of an organization, which may provide false information about the scheme.

6. A solid investment opportunity should stand on its own merits and not rely on purported associations with well-known persons or entities.

7. Do not rely upon or make assumptions about the use of names and reputations of alleged backers or prior investors without further inquiry and investigation; know your counterparty.

8. In countries or situations where it is difficult to investigate secret personal relationships with powerful people and organizations, extreme caution should be used by a prospective investor.

9. Do not rely on a business card as a means of identification of the individuals with whom one is dealing.

10. Professional intermediaries must also be aware of the dangers of relying on the use of names without an independent investigation.

11. Organizations should actively and publicly defend their name and expose any improper use of it and should make publicly clear the organization's legitimate functions.

D. Additional references

Indicator 1. Irregular documents; Indicator 6. Undue secrecy; Indicator 8. Frustration of due diligence; Indicator 10. Psychological inducements and ensnarement; Indicator 15. Fraud based on abuse of personal affinity or relationships; Indicator 17. Unusual involvement or participation of professionals; Addendum 1. Performing due diligence.

Indicator 5. Disproportionate returns

1. Commercial frauds often guarantee yields with little or no risk.

A. Explanation

2. Every investor wishes to maximize returns. However, it must be remembered that returns are always proportionate to the perceived risk, which varies amongst investments. When the risk is high, investors require higher returns than they would receive from less risky investments before placing their capital at risk. Therefore, the higher the risk, the greater the promised return. In order to induce investments, commercial frauds distort this principle of proportionality, promising returns which are disproportionately high for little or no risk. Often promised returns are even far in excess of what could be earned from highly speculative investments. The risk-free character of the proposed investment is emphasized using a variety of means, including promises or guarantees from the fraudster or from third parties or entities. Some fraudulent schemes purport to provide evidence that the returns are being earned or they may even actually pay such returns from the money originally invested or from money invested by other investors, so-called "Ponzi" schemes.

B. Instances and examples

3. Commercial frauds promise:

(a) Low risk;

Illustration 5-1: The literature in support of the investment provides assurances that the principal or principal and earnings are "risk free" or "without risk".

Illustration 5-2: The funds are said to be in an account that is under the control of the investor and that the funds will not be moved without the investor's permission.

Illustration 5-3: Phrases such as "riskless principal" are used out of context.

(b) Guarantees are made or given;

Illustration 5-4: The fraudster provides a personal guarantee or one from an accomplice, but such a guarantee is worthless.

Illustration 5-5: The fraudster promises a guarantee from a major bank or financial institution which will be provided when the investment is made.

Illustration 5-6: The fraudster indicates that the funds or investment are insured.

Illustration 5-7: The fraudster asserts that the funds are guaranteed by a governmental or international agency or organization.

(c) Or disproportionately high or consistent returns.

Illustration 5-8: The returns promised frequently range from 20 per cent per month to 50 per cent per month in a low inflation currency, or unrealistically consistent returns given the market rate.

4. The disproportionately high returns are explained in a variety of ways.

Illustration 5-9: High returns are justified by the volume of "trading" in which small profits per trade are accumulated. Usually the mathematics supporting these figures is flawed: the calculation may fail to take into account expenses, or may suggest more trades than typically take place in the given investment.

Illustration 5-10: Sales and market data are often manipulated, especially with respect to the time frame, to make it seem that returns are very high over a very short period of time.

5. Note: Even the actual payment of promised high returns does not ensure the legitimacy of the investment.

Illustration 5-11: Alleged returns may be paid from the investor's own money or that of other investors and not from any real return on the investment, as in the case of a "Ponzi" scheme.

Illustration 5-12: Such high returns often appear only as bookkeeping entries and investors are encouraged to "reinvest" by the promise of even higher returns.

C. Advice

6. If an investment scheme sounds too good to be true, it probably is not genuine.

7. Perform due diligence by understanding the nature of the investment, its likely and possible risks and returns or consulting with an independent person who may be relied upon to provide appropriate advice.

8. Beware of confidence builders, i.e. small, insignificant transactions which appear effective and offer suitable returns aimed at inducing further and more substantial investment.

9. Excessive emphasis by a promoter on rate of return, or that an investment is "no risk" or "low risk" or "high return", with little or no discussion of the substance of the investment should be a cause for concern.

10. The returns promised are completely out of proportion to the risk assumed and to prevailing market rates of return.

D. Additional references

Indicator 8. Frustration of due diligence; Indicator 9. Abuse of incentives; Indicator 13. Questionable or unknown source of repayment; Indicator 15. Fraud based on abuse of personal affinity or relationships; Indicator 20. Pyramid and multi-level marketing schemes; Addendum 1. Performing due diligence

Indicator 6. Undue secrecy

1. Commercial frauds frequently seek to impose undue secrecy and confidentiality on a number of issues including the existence of the opportunity to invest, the nature of the investment, the investment mechanisms and the source of return.

A. Explanation

2. Transparency is critical to the functioning of modern financial markets and information about these markets and investments is widely available. On the other hand, investors do engage in investments based on confidential information or information whose significance is not widely understood. In some situations, acting on such information can be illegal. In other commercial activities, companies legitimately seek to prevent disclosure of confidential information or industrial techniques by employees or others by various legal devices in order to remain competitive in an industry. Such restrictions however, are almost never appropriate with respect to investors and particularly not with regard to the means by which funds are to be generated. Undue secrecy is a level of secrecy that goes beyond that which is appropriate to the transaction.

3. The requirement of secrecy may be set out in rules or requirements, often coupled with "legal sanctions" purporting to make investors liable for damages should they disclose any information, in order to suggest that the financial decision maker would be implicated, should the transaction be revealed. Such secrecy is intended to obscure the transaction, to inhibit the exercise of due diligence and to prevent investors from contacting advisors or appropriate sources of information that might assist the investor in avoiding the fraud.

B. Instances and examples

4. Multiple excuses are given to justify undue secrecy.

> *Illustration 6-1:* Frequently, it is claimed that consulting with knowledgeable persons or organizations disrupts the business transaction, interferes with the deal somehow, and ruins the opportunity for profits.
>
> *Illustration 6-2:* Claims are often made that banks, stock markets, CEOs, professionals or prominent persons engage in the type of investment at issue on a regular basis, but secretly, in order to prevent the public from gaining a similar financial advantage.
>
> *Illustration 6-3:* It is often claimed that the laws of off-shore jurisdictions that are somehow connected to the investment require such secrecy.

5. During the course of the transaction, victims are often warned against contacting the police, regulators or other officials.

> *Illustration 6-4:* It is often stated that the involvement of regulators will cause the transaction to be frozen, delayed or jeopardized, placing the onus on the victim.

6. The term “Non-Circumvention or Non-Disclosure” is frequently used in connection with attempts at secrecy. Such provisions are used in businesses where there is a middleman linking buyer and seller, but are completely inappropriate or of concern with respect to ordinary investments.

> *Illustration 6-5:* Victims are required to sign a detailed ICC (International Chamber of Commerce) Non-Circumvention and Non-Disclosure Agreement that, if taken at face value, would prevent them from discussing the investment with their accountant, attorney, or financial advisor.

7. Confidentiality or secrecy is often given as an excuse for the lack of public information about the investment.

> *Illustration 6-6:* Illogical claims that allegedly prove the genuine nature of the transactions, such as that the United States Federal Reserve chairman knows about this type of transaction, but if asked about it, he would deny it.

8. Sources of concern include the following in a financial as opposed to a commercial transaction:

> *Illustration 6-7:* Repeated insistence on absolute secrecy.

> *Illustration 6-8:* Investors are required to sign agreements with disproportionately serious sanctions should they disclose information.

C. Advice

9. Investors should discuss the proposed transaction with a competent professional advisor.

10. An investor should ask whether there is any commercial imperative for the secrecy or whether the secrecy is unrelated to the core concept of the investment.

11. An investor should not be intimidated by the suggestion that liability will result from revealing aspects of the transaction to financial advisors.

12. An investor should remember that legitimate confidentiality agreements do not prevent or forbid either the performance of due diligence on the transaction, or the contacting of authorities.

13. An investor should not participate in investments when funds are moved offshore unless complete and detailed information on the transaction is available in order to ascertain where money is flowing and whether movement of funds to that jurisdiction could be improper.

D. Additional references

Indicator 1. Irregular documents; Indicator 2. Misuse of technical terms; Indicator 4. Misuse of names; Indicator 8. Frustration of due diligence; Indicator 9. Abuse of incentives; Indicator 10. Psychological inducements and ensnarement; Indicator 12. Immediate, fast or irrevocable transfer of funds; Addendum 1. Performing due diligence.

Indicator 7. Overly complex or overly simplistic transactions

1. Commercial frauds are often designed to be overly complex in an attempt to obscure the fundamentals of the transaction, and may include illogical representations as well as convoluted, circuitous or impenetrable documentation. On the other hand, some commercial frauds may also be unduly simplistic or informal, with very little documentation or explanation, despite their apparent connection with a sophisticated or complex financial transaction.

A. Explanation

2. Although commercial transactions, particularly international commercial transactions, may at times be complex by their very nature, the person being asked to make a decision with financial implications should have at least a basic understanding of the transaction in which participation is being solicited. Fraudsters often use as a model legitimate transactions that are highly complex and therefore marketed only to very sophisticated investors. This model is then used by the fraudster to involve less sophisticated individuals who may not be capable of understanding the nature of the transaction or the necessity of the complexity. Further, a web of companies or other entities may be created in order to distance the fraudster from blame when the fraud is discovered, to frustrate asset recovery, to launder the proceeds of crime, or to enable the fraudster to continue to operate a series of parallel schemes. Artificial or unnecessary complexity and absurd oversimplifications are two techniques that fraudsters use to obfuscate the fundamentals of the transaction, which, typically, make no economic sense.

B. Instances and examples

3. Inordinately complex business structures that create a façade for multiple companies with no apparent role or reason are designed to make it difficult to hold fraudsters accountable.

> *Illustration 7-1:* Six individuals formed a number of corporations and companies under the umbrella of a "programme of empowerment" and "wealth enhancement" network, conducting large workshops to entice unsophisticated investors into investments in foreign currency that they falsely described as highly profitable and "low risk".

4. Very little documentation may be associated with an unduly simplistic or informal transaction that would ordinarily require significant documentation.

> *Illustration 7-2:* Homeowners in imminent risk of foreclosure were persuaded to sign a simple form to "temporarily" transfer ownership

of their homes to “straw buyers”. The straw buyers then applied for mortgages on the homes using phoney credit histories. After draining the equity, the loans were defaulted upon, subjecting the owners to threats of eviction. The financial institutions recovered little.

Illustration 7-3: The presence of highly informal text in the documents, for example, the use of a phrase such as “telephone at the usual number”, may signal the presence of a commercial fraud.

5. Complexity compounds problems related to tracking payments and disbursements and recovering funds.

Illustration 7-4: Frequently, fraudsters use multiple layers of business entities to conduct multiple transfers of funds and/or frequent changes of depositary banks. Since transnational fraud schemes also often use Internet-based funds transfer mechanisms rather than conventional banking channels, such funds are extremely difficult to trace.

6. Technology, including transportation, information and communication technology, is increasingly being used to inject complexity in order to avoid detection and to conceal proceeds.

C. Advice

7. Be aware that there may be commercial fraud when there is no explanation and no apparent commercial purpose for complexities in the transaction, where intricacies appear artificial, where there appear to be parties with no meaningful role, or where the number of transactions or transfers or the structure of the transaction make it difficult to investigate it.

8. Ensure that the purpose of each element of the transaction is understood. Do not be afraid to ask questions, even though it is possible that the answers might be obvious.

9. Legitimate transactions may be complex, but, if so, they require informed counterparties using independent advice from knowledgeable sources.

10. If details cannot be provided immediately, it should not deter the investor from obtaining the details from elsewhere prior to investing.

11. Inquire into who initiated the transaction, who is recommending it, who is promoting it, and why a particular individual was approached as a potential investor. When there is an apparent effort to discourage questions from being asked, be suspicious of the reasons.

D. Additional references

Indicator 8. Frustration of due diligence; Indicator 10. Psychological inducements and ensnarement; Indicator 19. Misuse of technology and electronic fraud; Addendum 1. Performing due diligence.

Indicator 8. Frustration of due diligence

1. Since due diligence is the key tool through which suspicions can be explored and suspicious transactions avoided, it is a primary goal of fraudsters to frustrate the proper exercise of due diligence.

A. Explanation

2. The person or entity being asked to make a decision with financial implications should ensure that due diligence is conducted through independent sources to investigate the proposed transaction, particularly any unusual aspects. The person being asked to invest should have the greatest motivation, and be best-placed, to conduct due diligence. Commercial frauds employ a wide variety of devices to frustrate the exercise of due diligence, whether by creating distractions; by creating false credibility through the impression of mass approval; by controlling the means by which due diligence is exercised; by directing the investor towards nonindependent sources; through the use of high-pressure sales tactics; through insistence on urgency or secrecy; or the like. Any attempt to thwart the complete and independent investigation of the transaction and especially unusual or questionable aspects is highly suspicious.

B. Instances and examples

3. A fraudster may attempt to prevent the exercise of due diligence by:

(a) Presenting information in support of the transaction that cannot be verified;

Illustration 8-1: A fraudster may suggest that eminent persons who cannot be contacted are involved with or have approved the transaction, or that the roots of the transaction lie in historical private or international agreements.

(b) Insisting on absolute secrecy;

Illustration 8-2: The fraudster promotes an investment to the potential victim but tells the potential victim that the investment and promised returns are only possible if absolute secrecy is maintained.

Illustration 8-3: The fraudster may claim that information used in promoting the investment is proprietary, secret, or confidential, and cannot be shared with independent sources for due diligence.

(c) Using high-pressure tactics;

Illustration 8-4: The fraudster insists that there is only a "short window of opportunity", or a "last chance" to invest before the opportunity is lost forever.

Illustration 8-5: The sense of immediacy may be tied to unrelated but current world events or crises, such as political upheavals or natural disasters, in order to increase the pressure to invest quickly.

(d) Insisting that due diligence is unnecessary;

Illustration 8-6: In a situation where the fraudster controlled all parties to a transaction (the buyer, seller and shipper), the buyer sought a letter of credit from its bank in favour of the seller. Although the goods did not even exist, the fraudster created forged documents that stated that the goods had been delivered, and sought to draw on the letter of credit. To persuade the bank employee to issue the letter of credit, the fraudster persuaded the employee that he had spoken to the employee's boss, who approved the transaction and the letter of credit, and the fraudster suggested that therefore the employee did not even require proof of ownership of the goods.

Illustration 8-7: A fraudster promotes a high-yield investment programme assisted by a lawyer and an accountant. Attendees at a seminar touting the investment programme hear presentations by the lawyer and accountant who claim to have examined the transaction and found it to be legitimate. Attendees are led to believe that the lawyer and accountant are independent, but they are each co-conspirators in the scam.

(e) Suggesting that the transaction has gained the approval either of the public or officials in the field;

Illustration 8-8: The fraudster promotes a high-yield investment programme to the potential victim and invites the potential victim to a seminar where the potential victim can learn more about the programme. The potential victim is taken to a seminar with hundreds of other potential investors. At the seminar, the fraudster touts his or her wealth, and may use the additional technique of promoting an association of the programme with well-known public figures, even if in a general way. All of these techniques generate a sense of mass approval intended to dissuade the victim from performing proper due diligence.

Illustration 8-9: Fraudsters can use any type of media, including print and electronic media, e-mail, television, live presentations, and the creation of convention-like events, to create a sense of mass approval of a certain "opportunity", in order to distract the victim from performing due diligence.

(f) Suggesting that due diligence is being performed and therefore it is unnecessary for the investor to do separate due diligence;

Illustration 8-10: A fraudster can give the impression that due diligence is being exercised when it is not by claiming that it is being undertaken by a third party, or by insisting that a guarantee, an escrow account, or some sort of outside professional involvement affords sufficient protection to the investor.

Illustration 8-11: A fraudster may recommend a specific professional to carry out the due diligence, but that professional has either been compromised by the fraudster, or has insufficient knowledge to carry out thorough due diligence.

(g) Or making due diligence impossible to accomplish, even while suggesting that the investor perform his or her own due diligence.

Illustration 8-12: A fraudster may encourage the potential investor to perform due diligence, but may effectively block its performance by providing incorrect or compromised contact information, creating excuses why key people cannot be contacted, providing insufficient detail regarding the transaction to perform the due diligence, and the like.

4. Commercial fraud may be signalled where there is unusual difficulty in obtaining additional and independent information on the transaction or the parties, due to their identities, to their geographic location, or to other factors.

Illustration 8-13: Fraudulent transactions often involve international companies based off-shore, making due diligence more difficult.

5. A fraudster may steer the potential victim toward non-independent sources of information when due diligence is being pursued, or may present false documents to bolster credibility.

Illustration 8-14: Fraudsters will use different means to frustrate due diligence, including setting up collaborators for the victim to call to verify information, and they have even been known to create elaborate sham businesses with actual premises when pursuing large investments from victims.

C. Advice

6. It is absolutely essential to seek independent and suitably qualified advice from sources other than those provided by the person encouraging the investment.

7. The person from whom advice is sought should be knowledgeable about the subject matter.

8. The key facts of the transaction should be verified.

9. Trust one's common sense and investigate thoroughly when an aspect causes one to feel uneasy.

10. Be aware that modern commercial fraudsters often work in sophisticated groups that loosely corroborate and reinforce one another and the scheme.

11. Evaluate the reasons for the immediacy, if any.

12. Take time to investigate and do not rush into a business decision, especially when the decision is regarding something out of the ordinary course of one's business.

D. Additional references

All other indicators. Effective due diligence is in all cases the key to avoid becoming a victim of fraud; Addendum 1. Performing due diligence.

Indicator 9. Abuse of incentives

1. Commercial frauds may involve taking advantage of an entity's performance incentives or offers of assistance, gifts, favours or other inducements to particular individuals in exchange for consideration that would not otherwise be available, or to overlook certain questionable activity.

A. Explanation

2. Performance incentives designed in accordance with international and national laws, professional ethics and industry standards can be a useful tool for encouraging profitable performance, particularly when they are subject to rigorous oversight. However, they can also mask fundamental problems with an account or a relationship, or give employees strong incentives to ignore what might otherwise be troubling signs.

3. Unless properly communicated, reported upon and monitored, even the best-intended employee incentive programmes weaken an entity's protection from commercial fraud. In addition to the possibility of employees themselves engaging in fraudulent activity to obtain incentives from their employer, outsiders may corrupt otherwise legitimate employee incentive programmes by seeking out poorly-managed schemes and targeting employees prepared to exploit those weaknesses.

4. Another aspect of the abuse of incentives in general is the use of gifts, status, favours, money, data, information or other inducements to create a conflict of interest for the recipient. By using such means to persuade senior management or other employees to engage in practices that are contrary to the generally accepted standards of prudent operation, fraudsters may use incentives to undermine the organization as a whole. What is sought can range from general amenability to help or to encourage the recipient to do something specific that is not improper in itself, but that facilitates something that is improper, to inducements that result in the recipient becoming a collaborator in the scheme.

5. Fraudsters may also mirror business incentives as a device in the course of their schemes: for example, by offering early investors financial incentives to recruit others in pyramid schemes, where payments are made from other participants' money. Fraudsters often use such incentives to persuade participants to "roll over" or reinvest illusory profits rather than be paid.

B. Instances and examples

6. Employees or fraudsters will take advantage of poorly monitored corporate performance incentives, for example, to enter into continuing transactions even when such transactions seem suspicious.

> *Illustration 9-1:* One hedge fund executive lost several hundred million dollars of investors' funds and deceived them and related institutions for more than three years using fake account statements.

7. Gifts, status, favours, money, data, information or other inducements that may create a conflict of interest for the recipient are intended to cause the recipient to give consideration that would not otherwise be available or to overlook or examine things that would otherwise be suspicious or problematic.

> *Illustration 9-2:* To curry favour, lenders provided all-expenses-paid trips for university financial aid officers and put university officials on their boards. Many universities operated as trusted middlemen by recommending these "preferred lenders" that did not necessarily offer the best rate to student borrowers.

8. Internal and external incentives and gifts may signal corruption or fraud in certain identifiable ways.

> *Illustration 9-3:* An employee is meeting very high performance expectations, with little oversight or understanding of transactions.

> *Illustration 9-4:* Unusual hospitality or excessive professional fees or excessive consultants' fees are offered.

> *Illustration 9-5:* A businessman well-known for generosity gave very expensive gold watches to bankers and lawyers that made it difficult for them to ask uncomfortable questions about the large loans that he took out and ultimately defaulted on.

9. Commercial and financial decisions should be made on their own merits.

> *Illustration 9-6:* The person whose influence is sought can be either the direct or indirect recipient of the gifts or favours, which may also be given to children, parents, spouses, etc.

> *Illustration 9-7:* The fraudster's goal is to obtain undue consideration or cooperation including obtaining contracts, information, documents, reducing the willingness to ask questions, providing access to people, compromising the integrity of the recipient or to encourage the recipient to become part of the scheme.

> *Illustration 9-8:* Scheme incentives typically include promises of unusual or excessive returns and strong encouragement to re-invest the windfall.

C. Advice

10. The oversight of employee incentive programmes should include review and audit by independent persons.

11. Systems should be in place to identify and resolve causes of employee grievances and to ensure that there are adequate and effective whistle-blowing policies.

12. Employers should have policy guidelines in place regarding receipt and reporting of gifts and favours, and should ensure that employees are aware of, and adhere to, those guidelines.

13. Professionals should be aware that they are often targets of attempts at improper inducements.

14. When receiving a gift, any employee or professional should consider carefully the value of the gift and the identity of, and relationship with, the giver.

15. Employers should ensure that purchases of gifts at company expense should be subject to review and approval by persons other than the donor.

16. Investors must understand how returns on an investment are generated, ask questions when cautionary flags are raised, and be open to seeking confirmation from an expert advisor.

D. Additional references

Indicator 5. Disproportionate returns; Indicator 6. Undue secrecy; Indicator 8. Frustration of due diligence; Indicator 13. Questionable or unknown source of repayment; Indicator 16. Fraud by or involving employees; Indicator 20. Pyramid and multi-level marketing schemes; Addendum 1. Performing due diligence.

Indicator 10. Psychological inducements and ensnarement

1. Fraudsters may seek to entice victims by using psychological inducements and manipulation first to persuade them into participating in the fraud, and then to ensnare them with respect to the real or imagined illegality of their participation in the fraud. Such ensnarement is then used against them to distract them or to obtain their silence regarding the much more serious commercial fraud being committed.

A. Explanation

2. Commercial frauds often use psychological inducements to encourage a financial decision maker to enter into a fraudulent transaction, and then to avoid detection of the fraud. An obvious inducement is an appeal to greed, but other factors can include fear of outliving one's savings; flattery of the decision maker, through gifts or references to investor sophistication; or the general appeal of being included in a private and exclusive deal. Many fraudsters can be very charming and persuasive people.

3. In terms of ensnarement, there is a natural psychological and moral reluctance to commit an improper or illegal action. Where an investor is induced to commit an act that may be questionable or illegal by a person seeking to involve the investor in an investment or other financial opportunity, this may be a device to ensure their silence or to distract them from the commission of a commercial fraud. Later attempts to avoid detection can include such psychological tools as threats regarding disclosure and suggestions of collusion or ensnarement.

B. Instances and examples

4. Fraudsters depend upon and prey upon powerful human emotions such as greed, pride, empathy or fear.

> *Illustration 10-1:* Potential victims are seen by the fraudsters as predisposed to believe there are secret ways to make enormous amounts of money with no risk.

> *Illustration 10-2:* While still in the enticement stages, a proponent of the investment appeals to the victim's ego by alluding to investment sophistication or by trying to make the victim feel foolish for asking for explanations of complex transactions or technical terms.

> *Illustration 10-3:* In many common financial frauds, cheques and money orders are made out for amounts larger than the debt owed or commission to be paid to the victim, so that the victim is induced to deposit the cheque or money order in his or her bank account and to

wire the balance of the funds to a foreign bank account before he or she is notified by the banks that the cheque or money order is counterfeit or invalid.

Illustration 10-4: Advance-fee fraud resorts to the victims' predisposition to cooperate with government regulations by inducing them to pay money to fraudsters for nonexistent "taxes", "fees" or "customs duties" before the fraudsters are expected to provide whatever goods or services (e.g., offshore tax shelters) they have promised to victims.

5. Commercial fraud schemes may be designed to appeal to certain psychological profiles by suggesting "secret" markets, conspiracies or exclusive business circles.

Illustration 10-5: Those who may be seen as distrustful of government are offered investments to avoid paying taxes through offshore accounts. In one multi-million dollar fraud, victims were offered 80 per cent annual returns through a secretive web of money dealers supposedly set up by a coalition of governments in 1914 to pay for World War I debt. The scheme claimed that seven "world traders" control the entire global money supply and act as a board of directors for a few hundred "licensed traders" around the world.

6. Promoters look for weaknesses in population groups, concentrations of immigrants, the poor, the elderly and the infirm, preying on emotions such as the fears of senior citizens running out of money.

Illustration 10-6: In a common scheme, information is received by the elderly that the recipient has won a large "unclaimed prize" or international sweepstakes drawing or lottery that must be claimed by submitting an advance fee or by calling a telephone or mobile phone number to which significant charges apply.

Illustration 10-7: Victims may be more at risk depending on their particular profile or their stage in life, such as whether they are elderly, recently divorced, have health problems, or may have recently won or been awarded a substantial amount of cash.

7. Some fraudsters use flattery and the veneer of sophistication to entice victims to participate in the fraudulent investment.

Illustration 10-8: The fraudsters may make a display of lavish lifestyles and expensive luxury goods as they offer sophisticated sounding but fictitious investment products that mimic the many new legitimate products, while counting on naïve investors not to ask questions to avoid seeming to be themselves unsophisticated.

8. When other psychological inducements fail, fraudsters often resort to inducing compliance by threat or actual use of violence.

> *Illustration 10-9:* Investors who have not realized they are victims are used to entice others to participate. When the fraud is discovered, these middlemen fear they, too, will be implicated, and the fraudster uses that fear to keep the middlemen quiet.

> *Illustration 10-10:* Once a victim discovers the fraud, the fraudster may threaten public embarrassment by exposing involvement in the scheme, or may string the victim along with a series of mythical difficulties, or may offer the potential of new schemes with even greater returns, all common tactics used to delay or deter disclosure of activities.

> *Illustration 10-11:* It may be suggested to an individual involved with the scheme, often a professional, that the professional has become a conduit for money-laundering, although perhaps unwittingly, and once implicated, the professional may be reluctant to report the scheme.

> *Illustration 10-12:* A major telephone service provider was threatened because a fraudulently activated phone had been shut off. In a recorded telephone call, the fraudster threatened the telephone service provider that if the provider did not provide access to its computer system, he would cause its web service to collapse through a denial of service attack—an attack designed to ensure that a website is so flooded with requests for information that legitimate users cannot access the website.

> *Illustration 10-13:* Fraudsters will try to frighten victims telling them that they are deeply implicated in the fraud and that they will not be allowed to escape the fraud, or that the fraudster has ways of seeing to it that they will be arrested by national or international law enforcement authorities. Witness intimidation is common in commercial fraud.

9. Fraudsters rationalize that there are no real victims because their targets are avaricious, complicit and gullible.

C. Advice

10. Try to objectively appraise the merits of the proposed transaction, and be aware that suspicions that flow from one’s own common sense appraisal should be taken seriously. Ask oneself “Why me? If this scheme really works, why

is some stranger in a hotel meeting room or on the telephone or the Internet approaching me with a complicated financial deal with such high returns with an offer to allow me to participate?"

11. One's ego should not override one's suspicions—keep asking questions, even though the scheme's promoter may intimate that one is foolish for not understanding. It is much more foolish to invest in something that is not completely understood.

12. Obtain legal advice from independent counsel with the competence to advise regarding the transaction.

13. Do not be discouraged from reporting a fraud to the authorities because of some ensnarement aspect.

D. Additional references

Indicator 4. Misuse of names; Indicator 6. Undue secrecy; Indicator 7. Overly complex or overly simplistic transactions; Indicator 8. Frustration of due diligence; Indicator 15. Fraud based on abuse of personal affinity or relationships; Indicator 17. Unusual involvement or participation of professionals; Addendum 1. Performing due diligence.

Indicator 11. Crisis-caused breakdowns in preventive controls

1. Commercial frauds may exploit weaknesses in control systems in order to take advantage of generous or emotional impulses in the aftermath of natural and man-made disasters.

A. Explanation

2. A hallmark of civilization is the exercise of generous impulses and actions towards those less fortunate. Natural and man-made disasters bring forth such impulses spontaneously. In response to recent hurricanes, floods, oil spills, typhoons, earthquakes and tsunamis, the public and private sectors of the international community have worked together and spent billions on recovery. The mass destruction of homes, businesses and public infrastructure and the displacement of millions of individuals require emergency action, characterized by trust in a common purpose. Commercial entities and transactions have a significant role in making possible support of disaster recovery by the private and public sectors. However, coincident with the common good, neither the presence of an emergency nor our natural crisis-driven impulse of mutual trust should take the place of understanding the investment or business transaction, or of the exercise of due diligence and vigilance in preventive controls. A key lesson of past disasters is that funding lost to fraud slowed the recovery effort and reduced the amount of support that could have been delivered to alleviate the suffering and needs of legitimate victims.

3. Fraudulent schemes anticipate that, in the aftermath of disasters, individuals, businesses and governments will tend to suspend due diligence or circumvent the operation of normal preventive controls. In the mental model of fraudsters, disasters create opportunities by opening or exposing control weaknesses at a time of enhanced national or international urgency and when there is a general heightened emotion on the part of populations wishing to place trust in a common purpose.

B. Instances and examples

4. The outpouring of public generosity in the immediate aftermath of a disaster is often manipulated by attempts to exploit charities or charitable giving.

> *Illustration 11-1:* There are always some fraud schemes involving solicitations for ostensibly charitable purposes. When natural disasters strike, the incidence of such schemes can rise dramatically. After terrorist attacks, or natural disasters like tsunamis, hurricanes

or earthquakes, for example, law enforcement authorities see a significant number of schemes that purport to be collecting money for first responders and survivors of the disasters.

Illustration 11-2: "High-yield" investment schemes spring up very quickly after major disasters or world events. Characteristic of such schemes are that the selling tactics are not aimed at a purely charitable purpose but mix the promise of great profits with alleged charitable or "humanitarian project" benefits. Often fraudsters allege that the scheme is "sanctioned by the United Nations" or that it is a "United Nations approved programme for investment".

5. As governments organize for response, fraudsters search for control weaknesses in their procurement, benefit and grant processing.

Illustration 11-3: Procurement fraud schemes, such as kickbacks from vendors to contracting agency employees in exchange for favourable treatment, occur with frequency in contracts for procurement of goods and services after large-scale natural disasters, when many governments and international agencies enter into contracts for debris removal and infrastructure rebuilding.

Illustration 11-4: Fraudsters pressure evacuees to give the fraudsters permission to receive their mail. Government disaster assistance cheques intended for the evacuees are sent to the fraudsters' addresses and then diverted to secure cash or buy goods from local businesses. Often the goods are then sold directly or through online auctions initiated by fraudsters in other regions, or even other nations, serving as "brokers" for theft rings in the immediate area of the disaster.

6. As private sector resources are accessed to engage in disaster recovery, fraudsters take advantage of information gaps in the damage assessment process and systemic breakdowns in controls normally associated with financial systems.

Illustration 11-5: Examples of insurance fraud include fraudulent claims for property damage or loss, or for feigned physical injury, and false claims for renovations due to disaster damage, as well as sales of false insurance contracts.

Illustration 11-6: Displaced financial institutions attempting to provide emergency banking services to disaster survivors experience an increase in cheque kiting: the use of several bank accounts in different geographic areas to make deposits and write cheques against the accounts before the deposit cheques clear the banking system, creating a "float" of money out of nothing more than the lag in time while cheques clear and post to their respective accounts.

Illustration 11-7: Fraudulent offers of business opportunities at reduced prices, or investment opportunities, often abound following natural disasters, such as offers to purchase property and invest in medical supplies or material for reconstruction.

C. Advice

7. Exercise any charitable impulses through appropriate and recognized charities.

8. Where there are claims that an investment will not only achieve high returns, but that it has the additional benefit of humanitarian purposes, disaster relief, or the like; or where such motives are held out as a basis for justifying investments or other financial opportunities that are not explicable or justifiable on their own business terms, there may be an indication of commercial fraud.

9. The sudden interjection of a commercial transaction in a non-commercial setting should raise concern that there is no real or logical connection between the charitable cause and the proposed scheme.

10. With a focus on substantially diminishing the opportunity for fraudulent access to systems through front-end controls, preventive controls are a key element of an effective fraud-prevention programme.

11. Well before any disaster, preventive controls should be field tested to ensure they operate as intended.

12. Repeat offenders are common in Internet-based fraud. Databases of prior fraud, as a defensive method, for example to compare elements of incoming orders to information in the prior-fraud database, may guard against repeat false orders or invoices.

13. A well-trained work force that is aware of the potential for fraud can help prevent fraud. Fraud awareness training with frontline personnel—specifically on the potential for fraud within the programme and the likely types of fraud they could encounter—is crucial to stopping fraud before it gains access into the business or government operation.

D. Additional references

Indicator 8. Frustration of due diligence; Indicator 15. Fraud based on abuse of personal affinity or relationships; Addendum 1. Performing due diligence.

Indicator 12. Immediate, fast or irrevocable transfer of funds

1. Commercial frauds often pressure potential investors not only to make a very rapid decision, but also to immediately or quickly transfer funds, leaving little to no time for due diligence or reliance on expert advice.

A. Explanation

2. Legitimate transactions often require quick decisions and immediate action. The individuals or entities engaged in such transactions typically have a prior understanding of the nature of the risks and rewards involved. Thus, those individuals and entities do not suspend due diligence in favour of quick decision-making, but instead, exercise due diligence of a different variety, or at different points in the transaction.

3. However, a fraudster will often persuade a victim of the need for quick decisions in an attempt to thwart due diligence or to effect an irrevocable transfer of funds in the fraudster's favour. A person or entity being asked to make a decision with financial implications may be pressured to effect immediate, fast or irrevocable transfers of funds in order to complete the transaction. Once sums have been transferred, they are easily further transferred by the fraudster, often into other international jurisdictions that may make retrieval or tracing difficult or impossible.

B. Instances and examples

4. The fraudster will insist on an immediate transfer of funds, leaving little or no time for even basic due diligence.

> *Illustration 12-1:* The promoter of an investment touts the investment's certain rewards and high yield. At the same time, the promoter will warn the potential victim that the investment opportunity "will not last", or is a "once in a lifetime opportunity", and that the victim must "act fast". The promoter insists on a quick decision before the victim has sufficient time to thoroughly review the transaction.

5. The immediacy of the transaction may be used to induce the victim to agree to additional terms.

> *Illustration 12-2:* An investor is induced to authorize a transfer to a new account established for the fraud. Because of an alleged need for urgency and convenience, the investor is induced to add the fraudster or his or her accomplice as a co-signer on the new account. The

fraudster and co-signer then transfer the funds in the new account into their control.

6. A fraud may also involve the immediate and irrevocable transfer of funds.

Illustration 12-3: A transaction involves transfers to an off-shore company described as an "anonymous" off-shore company, or to an off-shore company, trust, or account in a "tax-haven" jurisdiction.

C. Advice

7. Do not be induced to enter into a transaction before exercising the requisite due diligence because of pressure and time limitations.

8. Never relinquish control over banking or investment accounts.

9. Understand the reasons given for any transfer of funds, especially when a transaction involves multiple transfers.

10. Be particularly vigilant regarding transfers of money to another jurisdiction, especially off-shore jurisdictions which have secrecy laws and make any recovery of transferred funds extremely difficult and cost-prohibitive.

D. Additional references

Indicator 6. Undue secrecy; Indicator 8. Frustration of due diligence; Addendum 1. Performing due diligence.

Indicator 13. Questionable or unknown source of repayment

1. Commercial frauds often obscure the source of payment of alleged earnings or returns on an investment by referring to vague sources, foreign sources, uncertain sources, such as generic "trading programmes" (sometimes on "secret" markets), or by suggesting sources of payment in international jurisdictions without a regulatory scheme or from unregulated entities.

A. Explanation

2. Knowing and understanding the source of repayment, as well as compliance with documented procedures that ensure accurate, timely repayment of earnings and returns is essential to legitimate commercial transactions. In commercial transactions, genuine financial intermediaries possess sound principles of management, clear business models and documented and well-executed processes that are subjected to ongoing evaluation of efficiencies. Efficient repayment operations are conditioned on clear and known rules and accurate communications with trusted counterparties. Commercial transactions often require foreign sources of repayment, however, transactions typically do not include unexplained complexities, or use of inefficient repayment methods, or requirements that sources of repayment depend upon unregulated international jurisdictions. Nor would it be usual for an offshore or foreign source of repayment to be part of an otherwise wholly domestic transaction. The person or entity being asked to make a decision with financial implications must understand the business reasons justifying the underlying transaction, and determine the specific commercial reasons for any complexities, and must know, with certainty, the source of repayment.

3. Fraudulent schemes often entice prospective investors into not questioning the source or method of repayment by offering unusual financial incentives that are not related to the underlying transaction, or that have no commercial justification. Investors may be lured by an "enhanced rate of return" to accept a promise of repayment from an entity with no discernible business connection to the transaction. Often, part of a fraudulent scheme may depend on the investor agreeing to repayments transacted through jurisdictions regarded as secrecy havens. This "offshore source" feature subjects the victim to further manipulation: by agreeing to unusual sources of repayment in exchange for the potential to avoid paying any taxes on proposed returns, the investor becomes complicit in the scheme. Vague, uncertain or offshore sources of repayment are often used to keep investors in a state of doubt, so that a fraud is not noticed until it is too late.

B. Instances and examples

4. The true nature of a transaction will be obscured, will likely lack commercial purpose, and will have improbable characteristics, such as disproportionate returns.

> *Illustration 13-1:* "Historical bonds", or bonds that were once valid obligations of commercial or sovereign entities but that are now worthless as securities and only collected or traded as memorabilia, are said to be worth millions or billions of dollars based on third-party statements often referred to as "hypothecated authentications" or "hypothetical valuations", and are sold to unsophisticated investors at inflated prices far exceeding their value as collectibles.

5. Returns are claimed to be from purported sales of more of a commodity than is produced or available in the world.

> *Illustration 13-2:* The source of repayment is claimed to be gold, that is "collateralized" by fictitious "gold certificates" or "warehouse receipts", variously said to have been issued by obscure or non-existent offshore banks, or by major financial institutions, or even by well-known international organizations, representing gold bullion that, if true, would require more gold than produced in recorded history.

6. Repayments are sourced from other participants' investments or from a participant's own investment.

> *Illustration 13-3:* In one "pyramid scheme" a "trading company" sold bags of ants asking investors to breed the insects and bring them back for a 130 per cent return. Initially, the purchase money received from new investors was used to pay returns to the previous investors. Pyramid schemes reach critical mass, and collapse, when the source of funds from new investors is inadequate for repayment of prior investors.

> *Illustration 13-4:* After falling for "high-yield", "Prime Bank" investment fraud, victims are often approached by a second team of fraudsters with an offer of "fraud recovery" services. Small amounts are "recovered" in exchange for an "advance fee". The victims are then pressured for additional and more substantial fees, and promised "more complex" higher value recoveries. The source of all funds "recovered" by the second team is the victims' own funds in the hands of the first team. The fraud continues until the second team has extracted all the fees the victims are willing or able to pay. By this time, the victims will have lost all funds initially "invested" with the first team and all "advance fees" paid to the second team.

C. Advice

7. Be able to identify the commercial purpose of the transaction and understand how the returns are generated.

8. An overemphasis on esoteric details, such as "historical bonds", overly complex methods of payment, inconsistent explanations regarding sources of repayment and unusual requirements predicate to earnings, are not typical of legitimate business dealings.

9. When returns are overdue an investor should immediately seek independent, objective advice and accept no excuse.

10. When a major source of returns is derived from inducing others to invest and, in turn, recruit others, great care must be exercised regarding the legitimacy of the scheme. If the major commercial purpose is obtaining percentages of investments from lower tier investors, it could be a so-called "pyramid scheme".

11. Do not become so focused on the amount of the alleged returns on the investment that one forgets to focus on the source of those returns.

12. Be suspicious of repayment methods or sources that involve entities, jurisdictions or complexities having no discernable business justification in connection with the transaction.

13. References to "high yield" and "no risk" investments in "secret trading programmes" or "secret trading rooms" in "tax-free" or "bank privacy" jurisdictions signal that the transaction departs from commercial norms and that there may be no commercial source of repayment. If confronted with such terms, investors must aggressively conduct due diligence.

D. Additional references

Indicator 5. Disproportionate returns; Indicator 8. Frustration of due diligence; Indicator 9. Abuse of incentives; Indicator 10. Psychological inducements and ensnarement; Indicator 20. Pyramid and multi-level marketing schemes; Addendum 1. Performing ue diligence.

Indicator 14. Irrational or illogical aspects or explanations

1. Once an investment has been made, in an effort to prolong the fraud or to hide the proceeds, a fraudster often relies upon any available or superficially plausible reason to explain any aspect that is questioned. Often, these excuses or explanations will not bear close scrutiny and will reveal the commercial fraud.

A. Explanation

2. Modern commerce and finance has a rational and systematic character. Although it may sometimes be difficult to understand, there are always commercial, historical, systemic or other reasons for its features that can be understood and explained. Where there are irrational or illogical elements of an instrument or scheme, particularly with respect to failed performances, further investigation is warranted and an independent expert should be consulted.

3. A fraudster will frequently give inconsistent or illogical explanations to persuade the potential victim not to seek such advice, to prolong the fraud or to hide the proceeds of the fraud. The victim may be given illogical explanations that attempt to induce the victim to participate further in the fraud. Or, when the proceeds are delayed, the fraudster may claim that returns due the investor are delayed by natural disasters, current events or other such events that typically would not affect transactions of the type contemplated. The victim may also be induced to remain silent about the transaction based upon threats that reporting will delay payment or make payment impossible.

B. Instances and examples

4. Fraudulent transactions may involve illogical explanations as to counterparties' roles or identities in the transaction.

> *Illustration 14-1:* The fraud may involve unlikely connections in the overall scheme, such as a banking transaction with organizations that are not banks, such as the United Nations or the International Chamber of Commerce, or a private banking transaction with an international banking institution that does not conduct retail banking, such as the International Monetary Fund or the World Bank.

> *Illustration 14-2:* The fraudster may describe clients or counterparties whom the victim never meets. For example, a lawyer promotes a transaction in which a "client" will trade financial instruments as a member of a secret inter-bank market in these instruments, but the client is never identified or introduced to the victim.

5. Irrational or illogical aspects may appear in the very fundamentals of the transaction.

> *Illustration 14-3:* There may be a serious disproportion in the overall structure of the transaction, such as a relatively small transaction with a huge, powerful bank allegedly behind it.

> *Illustration 14-4:* Illogical logistics may appear, for example, in the sale of goods, where the movements of such goods do not make sense geographically in terms of where they are typically produced or grown.

6. Irrational or illogical explanations may also be used to explain delays in realizing the proceeds of a transaction. In most situations, the reason claimed for the delay bears little relationship to any actual or likely delay in the transaction.

> *Illustration 14-5:* The fraud may involve claims of delays falsely attributed to legal considerations, governmental interference, current events such as natural disasters or political changes. In one case, for example, the fraudster claimed that international payment systems were shut down after the death of a member of a royal family, and the proceeds of a transaction would not be available until after the systems had been reopened.

7. A fraudster may actively discourage reporting the current failure to complete a transaction or the failure to make payment by claiming that doing so will make future completion or payment impossible.

> *Illustration 14-6:* When proceeds are not realized, the fraudster may tell victims that realization of the investment is pending and that, if reported, the authorities will not understand the transaction and will cause unnecessary delays while they investigate it.

> *Illustration 14-7:* When a victim questions the fraudster about delayed proceeds, the fraudster may attempt to ensure silence by leading the victim to believe that he or she, too, is implicated in any fraudulent conduct. For example, the fraudster may admit to the victim that the transaction is of questionable legality but that because the victim had received some proceeds from other victims, he or she is just as guilty as the fraudster.

C. Advice

8. Think critically about the logic or likelihood of explanations, and when the explanations are not understood, do not be embarrassed or afraid to seek independent advice.

9. Always ask the promoter of a transaction to explain necessary terms or critical roles if they are not understood. Be suspicious of a promoter who cannot explain vital roles or terms satisfactorily, and be willing to seek objective advice in such cases.

10. It is better to face unpleasant suspicions and investigate them sooner rather than later, since time is always in favour of the fraudster.

11. If there is doubt, seek assistance from the authorities.

D. Additional references

Indicator 3. Inconsistencies in the transaction; Indicator 8. Frustration of due diligence; Addendum 1. Performing due diligence.

Indicator 15. Fraud based on abuse of personal affinity or relationships

1. Commercial frauds often take advantage of non-economic factors such as the natural trust between people of similar backgrounds to cause potential victims to reduce the due diligence that they would otherwise exercise and to use the group as a source of potential victims. Moreover, commercial frauds often tailor themselves to the beliefs or commonalities that unite or are characteristic of a group.

A. Explanation

2. It is normal to give credibility to and to defer to those with whom one is closely associated such as relatives, friends or those of similar backgrounds, including religious, social, political, ethnic, charitable, fraternal and other relationships. Commercial frauds often play on these affinities to promote themselves and cause investors to substitute the security of the affinity for understanding or seeking out advice with respect to the proposed investment. The problem lies not in the affinity or relationship, but in an excessive reliance on the common linkage instead of objective factors related to the proposed investment.

B. Instances and examples

3. Relationships that can be abused include:

(a) Family relationships;

Illustration 15-1: Fraudsters often induce relatives and friends to invest in a scheme of which they would otherwise have been sceptical.

(b) Sports teams or apparent celebrity endorsements;

Illustration 15-2: The fraudster uses the reputation of a major sports figure to induce and promote investments that are fraudulent.

Illustration 15-3: An eminent citizen or celebrity is invited to an event promoting an investment, and by accepting the invitation, appears to be personally endorsing the investment.

(c) Religious or cultural affinity;

Illustration 15-4: A religious or cultural group is encouraged by other members or a leader to join an investment scheme that purports to benefit their common faith or heritage only on the basis of that relationship.

Illustration 15-5: A group suddenly becomes focused on a particular investment or scheme, seeming to support it en masse, when it is unrelated to the purpose or common theme of the group.

Illustration 15-6: A previously unknown individual becomes a member of a particular group, becomes influential in the group, and strongly encourages a particular investment or scheme to members of that group.

Illustration 15-7: A sudden change in the group dynamic from a religious or cultural focus to a more commercially-oriented one.

(d) Or charities.

Illustration 15-8: A fraudster uses a current tragedy to set up a false charity whose proceeds benefit the fraudster and affiliates and not the victims of the tragedy.

Illustration 15-9: It is common for commercial frauds to state that a certain portion of funds will be used to benefit a given humanitarian or other charitable cause.

4. Assurances: The fraudster may attempt to link the fraud to the group to provide added comfort.

Illustration 15-10: Fraudsters may convince a group that funds invested will remain in the control of the group.

5. The credibility of these schemes can be enhanced considerably by returns paid as promised from the same money invested or the investments of others.

C. Advice

6. Trust based on shared interests or relationships should not take the place of understanding the investment or business transaction or of the exercise of due diligence and vigilance in protecting one's interests.

7. Think independently.

8. Do not substitute the friendly advice or suggestions of an acquaintance from a social or other group for professional advice when finances are involved.

9. Because a counterparty has had a history of financial solvency in the past, do not assume that it is necessarily solvent today.

10. Knowing one's counterparty must be an ongoing process, since circumstances can change, and business stresses can lead to reckless and fraudulent behaviour even in a previously legitimate business.

11. Do not allow outward trappings such as expensive cocktail parties at luxurious hotels, or meetings of like-minded individuals, to cloud one's judgment regarding a potential investment.

12. Be careful which invitations are accepted and thus those to which one's name and reputation are lent.

D. Additional references

Indicator 4. Misuse of names; Indicator 5. Disproportionate returns; Indicator 8. Frustration of due diligence; Indicator 10. Psychological inducements and ensnarement; Indicator 11. Crisis-caused breakdowns in preventive controls; Indicator 20. Pyramid and multi-level marketing schemes; Addendum 1. Performing due diligence.

Indicator 16. Fraud by or involving management and/or employees

1. Managers and employees (including corporate insiders with access to similar information or systems, such as agents, contractors, and affiliated companies and parties) of all levels can be involved in a variety of frauds ranging from obtaining a position of trust with a view toward perpetrating a fraud, to taking advantage of an opportunity or situation within an entity either alone or in concert with other employees or outsiders.

A. Explanation

2. All businesses operate through employees. Employees, however, have access to non-public information (including information that is confidential or proprietary) and are effectively placed in positions of trust. Commercial frauds are often accomplished with the involvement of employees of the entity that is being defrauded. Frauds may involve managers, employees with professional designations, outside consultants, highly overqualified employees in sensitive positions, poorly-vetted temporary employees, and senior or highly-experienced employees or chief executive officers who are perceived to be unchallengeable. Various frauds are possible, and may include the movement of funds, the acquisition and sale or inappropriate use of sensitive information, inventory fraud, procurement fraud, and accounting frauds to inflate assets or earnings. Motivations or opportunities for employee fraud may include overambitious performance targets, annual bonus or incentive programmes, grievances or lack of sufficient supervision or internal controls.

B. Instances and examples

3. Fraudsters may seek to place themselves or an overqualified employee in an easily-obtained but lower-level position in order to illicitly obtain information or other valuable data for various improper purposes.

> *Illustration 16-1:* Cleaning or maintenance staff having unsupervised access to sensitive information sells the information.

> *Illustration 16-2:* Temporary staff with decision-making power have access to valuable documents, steals and sells them.

4. An employee who does not have sufficient skills to perform when he or she is under-qualified for a position may feel pressure to commit fraud to achieve mandated performance goals or to appear to comply with performance expectations. Extravagant bonuses tied to unrealistic performance goals may motivate employees to participate in fraudulent schemes to achieve bonuses.

5. An unhappy employee or one who does not believe he or she is properly appreciated may engage in fraud or be a target for a fraudster to use in a fraud against the company.

> *Illustration 16-3:* A disgruntled employee seeks to punish a company by participating in a fraud.
>
> *Illustration 16-4:* A disgruntled employee may accept kickbacks or bribes to make up for perceived lack of appreciation.
>
> *Illustration 16-5:* An employee who feels unappreciated becomes involved in bid-rigging or price-fixing.

6. Employees may be tempted to use their ability to access business assets, including non-balance sheet assets such as customer lists, for their own purposes.

> *Illustration 16-6:* An employee may be making unauthorized personal use of business assets to enrich themselves—even low level fraud such as unauthorized telephone charges or access to office supplies can add up over time.
>
> *Illustration 16-7:* An employee may engage in expense account manipulation.
>
> *Illustration 16-8:* An employee without an understanding of the importance of data may be approached to sell seemingly insignificant information.

7. Employees may be requested or pressured by senior managers to assist in a fraud conducted at the company itself, or on behalf of the company for which they work.

> *Illustration 16-9:* A senior banker facilitated a multi-million dollar cheque fraud operation for the benefit of a personal friend, overriding the bank's internal controls by directing a junior employee to approve transactions while the senior banker was on holiday. In fear of losing his job if he refused, the junior employee acquiesced, and detection of the fraud was avoided.

8. The work of a senior employee or the chief executive officer may be perceived as too complex, too important or too lucrative for it to be challenged or examined, and any fraudulent activity thus remains undetected.

> *Illustration 16-10:* A multi-partner firm of lawyers was ruined by the activities of a dominant and apparently successful senior partner who was facilitating massive frauds.

Illustration 16-11: A very large firm of lawyers suffered reputational and financial damage in the millions arising from work by a partner which others often remarked upon as being odd but clearly too complex for them to understand.

C. Advice

9. Entities should use independent auditing committees, analytical review and surprise audits of both successful and unsuccessful aspects of operations.

10. Employers should create fraud and conflict of interest policies and should ensure that employees are informed of them and trained in their operation.

11. Employers should have effective whistle-blower policies in place, and ensure that employees are informed of them and have confidence in their operation.

12. Employers should ensure that all employees and senior managers are adequately supervised.

13. Employers should perform periodic reviews of company contracts and agreements to eliminate contract and procurement fraud, such as kickbacks, bribery and conflicts of interest.

14. Employers should ensure that no single employee possesses too many decision-making powers, and that there is an appropriate separation of important responsibilities amongst employees within an entity, as well as effective internal oversight.

15. Employers should impose mandatory vacations: employee fraud is often detected when the wrongdoer is not present to control the situation, and employee fraudsters often never take holidays or may work unusual hours in comparison with other employees in the company.

16. Employers should create periodic job rotation, provided it is consistent with local labour laws.

17. Employers should have employee assistance programmes to help employees deal with the pressures of dealing with issues such as addiction, family problems or economic hardship.

18. Employers should consider programmes to encourage loyalty amongst employees, including paying them competitive salaries.

19. Employers should be alert for sudden changes in an employees' lifestyle, including extravagant purchases or excessive lines of credit.

20. Employers should ensure that the knowledge and skill of employees are consistent with the position they hold.

21. Employers should check references or credentials in employment applications or resumes.

22. In general, employers must create a robust control environment in the business in order to prevent fraud.

D. Additional references

Indicator 8. Frustration of due diligence; Indicator 9. Abuse of incentives; Addendum 1. Performing due diligence.

Indicator 17. Unusual involvement or participation of professionals

1. The involvement of a professional does not guarantee that a transaction is necessarily genuine, particularly when the involvement seems unusual in some way.

A. Explanation

2. Commercial transactions naturally involve professionals in a variety of roles. Moreover, businesses rely on professionals for advice and to protect themselves from commercial fraud. They may use an attorney to draft the documents used in a transaction; an accountant to give advice regarding how a transaction should be recorded on the company's books or on its tax implications; or a financial adviser or a banker to recommend a particular transaction or to give advice regarding certain types of transactions.

3. However, where the professional's involvement in the transaction seems unusual, a commercial fraud may be indicated. Where the professional provides no advice or services, but simply transfers money, or where the professional performs acts typically performed by another type of professional, a fraud may be present. Fraud may also be indicated where heavy reliance is placed upon a particular professional who is provided by the promoter of the investment to the exclusion of independent advice or due diligence from an outside professional. In addition, an individual acting as a professional should have the proper education and experience to provide the advice or services expected.

B. Instances and examples

4. An individual who lacks proper credentials, or whose credentials cannot easily be verified, performs acts typically, or exclusively, performed by professionals.

> *Illustration 17-1:* A fraudster promoting an investment scheme provides potential investors with the testimony of an individual who verifies that the transactions in a particular instrument are legitimate. The individual is not presented as an attorney, accountant or financial adviser and holds no such credentials.

> *Illustration 17-2:* The professionals involved have a disciplinary history, possibly including customer complaints, civil actions, or criminal prosecutions.

5. The promoter of a transaction relies heavily upon, and advocates resort to, a particular professional working with the promoter, to the exclusion of independent advice.

> *Illustration 17-3:* A promoter assures potential investors that a transaction has been approved by an attorney named and advocated by the promoter, and encourages the investors to direct all questions to that attorney. The promoter may also state that other attorneys will deny the existence of the transaction, because they are not experienced enough to be aware of such transactions.

6. A professional may provide no advice in connection with a transaction but will simply hold or transfer money, and if the professional is an unwitting participant in the scheme, may receive handsome fees simply for holding or transferring money.

> *Illustration 17-4:* A party is informed that an accountant or lawyer will participate in a transaction, but the accountant or lawyer's only role is to accept money from that party and transfer the funds to the fraudster. The fraudster uses this arrangement to hide the sources of funds, and possibly to influence the professional by alleging his or her involvement in money-laundering.

> *Illustration 17-5:* The funds are said to be placed in an escrow account of a professional such as an attorney, which is intended to provide added confidence as to the safety of the investment and the funds. However, the professional may be negligently or deliberately assisting in the fraud or may be under the instruction of the fraudster rather than of the person depositing the funds.

7. A fraudster may use reputable advisers, but restrict their terms of reference or provide them with false or misleading information.

> *Illustration 17-6:* An independent lawyer or an accountant is engaged to assist on the transaction, but is provided with false financial statements and accounting records.

C. Advice

8. If in doubt about a professional, seek independent advice, such as one's own professional advisor who is known and trusted; never rely solely on advice given by professionals suggested by one's counterparty.

9. Never suspend due diligence solely because a counterparty's professional advisor claims to have found the transaction to be legitimate.

10. If a professional recommended by the promoter of the investment is involved in the transaction, check that professional's credentials and disciplinary history with any available licensing or regulatory authorities.

11. Professional indemnity insurance and fidelity funds often refuse to cover losses arising from frauds. Do not rely on such cover as a substitute for due diligence.

12. Professionals should question unusual instructions received from their clients.

13. Professionals who are sole practitioners or part of a small firm and are involved in apparently very high value transactions and receiving high fees for little or no services should question the purpose of their professional involvement.

14. Professionals should be careful of being drawn into transactions that they do not understand or are unsure about, particularly if they are offered unusual inducements such as a very high level of fees or overly generous hospitality.

D. Additional references

Indicator 1. Irregular documents; Indicator 4. Misuse of names; Indicator 8. Frustration of due diligence; Indicator 10. Psychological inducements and ensnarement; Addendum 1. Performing due diligence.

Indicator 18. Inappropriate requests for information disclosure

1. Commercial frauds often rely on information obtained using means or a manner that would be unusual or inappropriate in certain circumstances; such information may be used to perpetrate a fraud against the individual or entity from whom the information is requested or against others.

A. Explanation

2. The perpetration of commercial fraud requires that the fraudster gather information both to prepare the architecture of the fraud and in order to identify potential victims. To this end, customer lists of an entity may be sought in order to identify possible victims, or internal directories of the entity may be sought, which the fraudster may use to provide himself an identity, to lend the fraud credibility or to identify possible accomplices. The fraudster may also need documents, logos or trademarks produced by an entity to copy in order to steal the entity's identity. Further, the fraudster may seek to obtain vital personal identification in order to steal an individual's identity. Such information may be sought in person, or by means of e-mail, telephone or fax solicitations.

3. The circumstances under which such information is requested may be inappropriate or unusual so as to signal a possible fraud. The request may be inappropriate, because the information requested is not usually disclosed using the form of communication requested, or, in more extreme examples, the request may be for sensitive information that is never disclosed in the manner requested by the fraudster. The request may seem unusual, because it concerns information not typically disclosed to an individual in the fraudster's position, or the request may be a part of a pattern of unusual requests of the entity or individual. Further, the request may be inappropriate, because the person asked to provide such information is not in a position to make such disclosures. Theft of information and identity fraud is a growing problem, for both individuals and organizations, and persons involved in commerce or finance should value information and should carefully consider any information disclosures that are requested.

B. Instances and examples

4. A fraudster may request information to be supplied in a manner not typically used to supply such information, or technology may be used to inappropriately access confidential information.

> *Illustration 18-1:* In a "phishing" scheme, a fraudster copies an entity's website or trademarks and sends an unsolicited e-mail to potential victims using the copied material to trick the victim into believing

the entity has sent the e-mail. The fraudster asks the potential victims to fill in sensitive personal information, such as bank account numbers or personal identification details and reply. The fraudster then uses the information to steal from the victims' accounts.

Illustration 18-2: Information stored or conveyed using technology may be subject to inadvertent disclosure, since personal organizers and mobile phones can be connected to computers to access information, and wireless technology is highly vulnerable given easily obtainable scanning equipment. "Keystroking" devices or software (or "malware", malicious software designed to access a computer system without the owner's consent) may be used to record and sift every keystroke made on personal computers, or to gather sensitive information in general.

Illustration 18-3: Aggressive telephone solicitations may purport to be promoting disaster-related relief, technologies or products (external or internal) in an effort to gain sensitive personal information.

5. The request may be for information that the entity or individual does not typically supply to individuals in the fraudster's position.

Illustration 18-4: Commercial frauds often involve requests for seemingly innocuous information, which an entity typically would not provide to customers or other individuals outside the entity. For example, the fraudster may request customer lists, internal telephone directories and the like, which the fraudster may use to contact potential victims or to impersonate the entity's employees.

Illustration 18-5: An entity is requested to provide an explanation of an entity's product or service on that entity's letterhead. The fraudster then uses the entity's letterhead to impersonate the entity or lend credibility to his or her scheme.

Illustration 18-6: An attorney is asked to verify that a client or business associate is familiar to the attorney or that the client or business associate is trustworthy. The client or business associate, a fraudster, then shows the letter to potential victims so that they are induced to invest with the fraudster.

6. A request may also be unusual, because the individual asked to disclose information is not in a position to make such disclosures.

Illustration 18-7: Fraudster requests that a bank teller issue a letter indicating that the fraudster has deposited with the bank "good, clean funds of a non-criminal origin". The teller, believing the requested statement to be true, issues what is believed to be a harmless letter, which the fraudster then uses in an investment scam to give credibility to himself and to the fraud.

7. A fraud may be indicated where unusual patterns of access have been made to a corporate database.

> *Illustration 18-8:* A corporate database is accessed multiple times by individuals outside the company. A fraudster may access such information to create lists of potential victims or to steal the identities of the listed individuals.

C. Advice

8. Business entities should protect confidential information through the implementation of instructions relating to access to and use of confidential information and through careful training of employees who have regular contact with the public, as well as by limiting which employees have access to such information.

9. Where appropriate to protect confidential information, employees should be requested to sign confidentiality agreements to protect highly sensitive information.

10. Any unusual requests for information should be carefully considered before an entity or individual complies.

11. Only use secure means when conveying sensitive information, such as credit card or bank account numbers, and destroy or protect receipts or other documents bearing such sensitive information.

12. Entities should employ both effective monitoring processes and effective security processes to ensure that confidential information cannot be accessed by those outside the company and that the entity is aware of attempts at access.

13. Entities should ensure that effective computer data protection policies and procedures are in place to guard against hacking and computer misuse, that confidential information is secure, and that any attempt to override the policies is a disciplinary offence.

D. Additional references

Indicator 8. Frustration of due diligence; Indicator 19. Misuse of technology and electronic fraud; Addendum 1. Performing due diligence.

Indicator 19. Misuse of technology and electronic fraud

1. The significant increase in the commercial use of information and communication technologies worldwide has introduced a corresponding increase in frauds which target commerce and which take advantage of technologies to reduce risks and increase potential proceeds and the number of victims.

A. *Explanation*

2. Wire line telephones, wireless or cellular telephones, fax machines, electronic mail and the Internet are examples of technologies that are available in both urban and rural areas throughout the world, and which are heavily used in commercial activities. There is a relationship between the availability and use of information, communication and commercial technologies and commercial transnational fraud.

3. Information, communication and commercial technologies are used as tools to defraud victims and to transfer and conceal proceeds. Fraud imitates legitimate commerce, making variations of commercial practice likely to produce corresponding variations in commercial fraud over time, between countries or regions, and with respect to specific areas of commerce. The number of fraud victims, total proceeds of fraud, occurrences of transnational fraud and fraud involving technologies have seen an increase, corresponding to the increased use of technologies in commercial systems and the availability of technologies to offenders and victims.

B. *Instances and examples*

4. Technologies are used to update and to increase the effectiveness of paper-based frauds that may date back hundreds of years.

> *Illustration 19-1:* One type of advance fee "phishing" fraud known as "419" uses the Internet and electronic mail to develop contacts and to pursue victims. A "419" fraud is a computer version of an ancient "your friend is a captive" fraud, in which hundreds of letters would be sent to wealthy families offering to free an imaginary victim in exchange for an advance fee. Using computers, in "419" frauds a few individuals are able to send billions of unsolicited e-mails worldwide promising the release of captive fortunes, a share of which may be obtained in exchange for personal or financial information of the victims and the payment of an advance fee. The wealth of the victims is siphoned off and their identity and financial information may be used to carry out additional frauds.

5. A general sense of confidence in global commercial and payment systems is used to lull suppliers into inaction and to suspend normal credit and payment controls.

> *Illustration 19-2:* A supplier of industrial machinery receives a large Internet order from an overseas buyer. Excited by the amount of the sale, the merchant accepts several different credit card numbers as payment. The charges are authorized by the credit card authorization centre and confirmation numbers are received. The machinery is shipped. Two weeks later, the merchant discovers the credit card authorization centre has charged back the value of the purchase, citing fraud.

> *Illustration 19-3:* While the vast majority of commercial Internet transactions are consummated without incident, increasingly fraudsters will contract for goods using counterfeit or altered financial instruments, or unauthorized or stolen payment card data as payment. By the time the merchant becomes aware the payment has been rejected, the goods may have already been shipped, received and disposed of by the fraudster. Recovery of amounts lost is extremely difficult and generally not possible.

6. After initially contacting a company by electronic mail, a fraudulent buyer will offer a corporate cheque or money order or draft in excess of the sale amount and ask that the seller return the difference by wire transfer.

> *Illustration 19-4:* A wholesaler receives e-mail from a buyer who places an order for $25,000 worth of goods. The buyer claims to be with an established company with international operations. The wholesaler receives a "certified company cheque" for $50,000 and contacts the buyer by e-mail to report the "error". The buyer instructs the seller to simply deposit the cheque, keep the monies owed and wire transfer the balance to an outlet of a money-wire service. Cautious the cheque could be worthless, the seller waits until it clears the bank. Assuming all is well, the seller wire transfers the extra funds as instructed and ships the goods. Two weeks later, the bank reverses the $50,000 payment. The cheque was counterfeit and was not detected by the company named on the cheque until its monthly reconciliation was completed.

7. Fraudsters know that the Internet provides safe and efficient ways to market stolen goods.

> *Illustration 19-5:* Online auctions are used to sell merchandise that fraudsters have stolen or fraudsters may act as brokers for theft rings in different regions of the world that may directly ship stolen goods to auction winners.

8. The Internet attracts fraudsters who use new technologies to maintain anonymity.

> *Illustration 19-6:* Fraudsters worldwide use Internet "pharming", look-alike, false websites aimed at redirecting a legitimate website's traffic to a fraudulent website.

> *Illustration 19-7:* Technologies and transnational fraud are linked when fraudsters use call-forwarding, anonymous re-mailers and similar means in an effort to conceal their identities and locations and avoid tracing by law enforcement.

9. Technologies, including transportation, information and communication technologies are increasingly being used more effectively by fraudsters to share expertise from one region to another, to identify, contact and deceive victims, to avoid detection and to conceal proceeds.

> *Illustration 19-8:* A growing variety of fraud schemes depend substantially on technological elements and exploit technological vulnerabilities, including telemarketing fraud, Internet fraud, credit and debit card fraud and financial institution fraud. The more sophisticated transnational fraud schemes have tended to take advantage of cutting-edge developments in technology to reach potential victims, including cellular telephony, Voice Over Internet Protocol (VOIP) and Internet-based communication, including social media.

C. Advice

10. Be aware that the scope of fraud conducted through the Internet and related technologies and encountered by the commercial community is very broad, reflecting the full diversity of legitimate commercial activity, and that international orders are particularly susceptible in this regard.

11. Exercise caution when entering Internet sales transactions that involve high-value merchandise, which are often involved in Internet fraud schemes, including online auctions or online retail sales and credit card fraud schemes.

12. Insist on receiving the appropriate amount of money for a sale and do not wire transfer cash back to a buyer based on an "overpayment" that was not made in cash.

13. When cheques, money orders, drafts or similar financial instruments are used as payment, certified or otherwise, verify the amount and check the number and signature if possible using direct communication channels outside the

Internet and electronic mail. Inquire with the postal service or issuing bank to verify that the document numbers or amounts are legitimate.

14. Beware of common misuses of technology, such as e-mail "phishing", where victims are induced to provide their own identity or financial information to fraudsters masquerading as commercial or government authority figures, or "pharming" where identical but false websites redirect a legitimate website's traffic to a fraudulent website.

15. So-called "SMiShing" is becoming more common; where fraudulent text messages are sent to cellular phones, similar to phishing e-mails.

16. Remove business incentives of fraudsters by including business measures such as charging a small fee for services or for access to a website.

D. Additional references

Indicator 7. Overly complex or overly simplistic transactions; Indicator 8. Frustration of due diligence; Indicator 18. Inappropriate requests for information disclosure; Indicator 20. Pyramid and multi-level marketing schemes; Indicator 21. Frauds involving goods and services; Addendum 1. Performing due diligence.

Indicator 20. Pyramid and multi-level marketing schemes

1. A fraudster may seek to recruit new sales personnel to sell merchandise or financial products. The sales recruit will be asked to pay (or "invest") a fee to join the programme and will then recruit others, who will also pay a fee, from which the fraudster and the earlier recruit will receive commissions. The recruit will typically be promised large returns, both from the sales and the recruitment fees.

A. Explanation

2. Manufacturers and marketing companies typically establish distribution networks and recruit sales forces to service them. Some may offer incentives to sales recruits to recruit other sales personnel to work for them and share their sales commissions. Such a multi-level marketing structure may be legitimate, but fraudsters also use such arrangements to facilitate fraud.

3. The sales structure is essentially in the shape of a pyramid with the fraudster at the top and successive layers of salespersons or victims beneath him. The objective is to obtain as large a sales force as possible to maximize fees. Additionally, the fraudster may require the recruit, and his or her recruits in turn, to purchase large quantities of product that may prove difficult to sell if the sales territory is saturated with sales personnel. Typically, the fraudster and a very few early recruits at the top of the pyramid are enriched, while the later recruits lose most or all of their investment when the pyramid ultimately collapses.

4. Regardless of the underlying product, service, investment or programme, any "profit" is illusory and is paid as the result of the pyramid type scheme. Such "profit" represents only principal or invested capital returned to the investor from his or her own capital or funds contributed by other investor-victims. Transnational multi-level, mass-marketing frauds use multiple jurisdictions to conduct different aspects of the schemes and have been known to use communication technologies that create the appearance that they are located in other nations.

5. Pyramid and multi-level marketing schemes can include elements of "Ponzi" schemes (see indicator 5), which "pay" returns to investors from their own money or from money invested by other investors, rather than from any profits earned as a result of the investment.

B. Instances and examples

6. At times the structure of the pyramid is itself the incentive and induces victims to provide references for the programme.

> *Illustration 20-1:* For a fee, a merchandise distributor offered prospective distributors the opportunity to recruit new salespeople and receive direct and override commissions for each new salesperson recruited.

> *Illustration 20-2:* Marketing various products, a company offered prospective distributors direct and override commissions for recruiting salespeople under its supervision. The prospective distributor must agree to purchase a large quantity of goods, which may be resold to its salespeople. The company does not have specific retail sales targets and commissions are computed on wholesale sales. Additionally, the company will not accept the return of unsold merchandise.

7. At other times, fraudsters use multi-level marketing structures in the background, relying on the underlying offer to entice recruits while changing details of the enticement to suit different regions of the world, consumer trends and categories of victims.

> *Illustration 20-3:* A promoter of a high-yield, no-risk, exotic financial instrument "roll trading programme" offered wealthy prospective investors 100 per cent per month returns and "bonuses" for introducing new investors, who would also be entitled to bonuses for introducing others.

> *Illustration 20-4:* In a consumer-centered economy, a promoter used newspaper advertisements, telephone messages and "investment seminars" at hotels and shopping malls to contact new recruits to an investment that promised returns up to 2,500 per cent per month within three months and 62,500 per cent with in six months with "no risk".

> *Illustration 20-5:* In a developing economy, where the right of private ownership was relatively new, a promoter lured investors from new economy employees, offering "undivided interest" in remote teak tree plantations or unidentifiable or even nonexistent individual teak trees.

> *Illustration 20-6:* In a transitional economy, a promoter enticed unemployed urban citizens with promises of 60 per cent returns in exchange for the right to breed insects for medicinal purposes.

8. Conditions such as major economic development or transitions can generate substantial increases in pyramid type, multi-level, mass-marketing frauds, that seek to take advantage of the confusion between old and new economic principles and specific activities such as the privatization of State-owned operations.

Illustration 20-7: One nation attempting to make the transition from central to private ownership suffered extreme economic failure as a result of a series of nationwide, privately run, pyramid type lottery frauds.

C. Advice

9. When a programme requires the purchase of expensive inventory and marketing materials, contact the appropriate regulatory authority for information on the programme and perform basic due diligence considering the quality and cost of inventory, reputation of the supplier and the like.

10. Be wary of programmes that offer commissions or high rates of return to prospective investors for recruiting new investors, who may, in turn, recruit others.

11. It is a signal of potential fraud when the promoter offers only a token amount of product while promising large returns if the prospective investor increases the number of new recruits and the programme does not permit the return of unsold merchandise.

12. Pyramid promoters often offer "asset enhancement programmes". It is a signal of potential fraud when the promoter offers "above market returns" or programmes based on exotic financial instruments, investments or products to participants not familiar with the market for the underlying instruments, investments or products, when the programme is offered at what is billed as a "charity event" or "benefit", or when the programme requires an initial entry fee.

D. Additional references

Indicator 5. Disproportionate returns; Indicator 8. Frustration of due diligence; Indicator 9. Abuse of incentives; Indicator 13. Questionable or unknown source of repayment; Indicator 15. Fraud based on abuse of personal affinity or relationships; Indicator 19. Misuse of technology and electronic fraud; Addendum 1. Performing due diligence.

Indicator 21. Frauds involving goods and services

1. Commercial frauds involving goods or services are often facilitated by fraudsters who falsely represent the nature, quality, quantity or value of goods or services to be delivered or that are the subject of investment.

A. Explanation

2. Sales of goods, information and services are important components of international trade. Fraudsters often take advantage of these activities to commit fraud by entering into the transaction with no intention of performing their obligations, or by deciding to do so during the course of the transaction. The fraudster promoting the transaction may perpetrate fraud by seriously misrepresenting the goods, information or services involved, or the purchaser of a product, an investor, or someone relying on the receipt of physical goods may find that the goods are never received or never existed. If goods are received, those that are received or in which investment has been made may differ substantially from the representations of the fraudster, or from the specifications of the transaction. Goods may be of greatly inferior or little value, counterfeit, or may have been tampered with in such a way so as to significantly reduce their value. Similarly, a victim that has contracted for the receipt of services, and paid in advance, might never receive those services.

B. Instances and examples

3. The goods that are the subject of the transaction or investment may be of lesser quality or value than as contracted, or the goods may be counterfeit.

> *Illustration 21-1:* Goods such as luxury products, art, antiques or precious stones, in which a buyer needs special expertise to ascertain their value or their provenance may be misrepresented as being much more valuable than they are or as having a legitimate provenance.
>
> *Illustration 21-2:* Fraudulent investments have been sought on the basis of an alleged massive projected increase in value of a variety of products, including art, stamps and even malt whisky.
>
> *Illustration 21-3:* Labelling may be changed or affixed to counterfeit products so as to pass them off on unsuspecting purchasers.
>
> *Illustration 21-4:* Pharmaceuticals or other products sold at greatly reduced rates on the Internet and elsewhere may not be genuine products, or they may be black market products being sold to gain proceeds from theft or other crimes.

Illustration 21-5: A fraudster contracts with a buyer for the sale of specifically manufactured goods. After the fraudster has received payment, the buyer discovers that the goods shipped are imitations.

4. A fraudster may represent that goods have been shipped or received when, in fact, they have not, or the fraudster may represent that goods exist when they do not.

Illustration 21-6: A fraudster contracts with a buyer to sell the buyer certain goods and both agree that the seller will accept a letter of credit as payment. The seller ships nothing but presents conforming documents to its bank, indicating that goods have been shipped, and the seller's bank pays the contract price.

Illustration 21-7: A fraudster seeks financing from a bank for the manufacture of raw materials into a final product. The fraudster represents that it is already in possession of the raw materials and induces the bank to finance the fraudster, although the bank has never observed the raw materials. The fraudster receives the proceeds of the transaction, although the raw materials do not exist.

5. The goods that are received may have been tampered with by the fraudster.

Illustration 21-8: A fraudster contracts to sell certain goods to a buyer, and both parties agree that seller will accept a letter of credit as payment. The fraudster ships the goods in containers, properly marked in conformance with the shipping documents. The fraudster presents conforming documents to the bank to receive payment, based upon delivery of the containers before the buyer discovers that the containers have been packed with scrap metal instead of the contracted goods.

Illustration 21-9: Seals on trucks or on containers of products may be tampered with, the contents of the truck or container removed, and the seals replaced with fraudulent seals.

6. The sale of information can also be fraudulent.

Illustration 21-10: A fraudster sells information from a database, but the names and addresses are false.

C. Advice

7. Before entering a transaction relying on the existence of goods, always ensure that the goods exist as represented.

8. Never blindly rely on the self-professed expertise of the promoter of the product, particularly when dealing with goods outside one's personal expertise.

9. If products are available for inspection, examine carefully the labelling and quality, or where necessary, have the products examined by a reputable expert.

10. When the commodity offered is significantly below its wholesale price, be suspicious: obtain a random sample and have it analysed or appraised by a reputable expert.

11. Know one's counterparty, including performing any due diligence necessary to establish the reliability of the counterparty.

12. Ensure that the amount of the good on offer is consistent with the production capabilities of the manufacturer, e.g. a small winery will only be able to release a limited number of bottles per year.

D. Additional references

Indicator 3. Inconsistencies in the transaction; Indicator 8. Frustration of due diligence; Indicator 19. Misuse of technology and electronic fraud; Addendum 1. Performing due diligence.

Indicator 22. Securities fraud and market abuse

1. Commercial frauds often involve the sale of securities that are not registered, sale by persons who are not licensed to sell them under applicable securities laws and regulations, or where market abuse or manipulation occurs.

A. Explanation

2. The issuance and sale of securities is an essential component of modern finance and commerce, and securities market regulators in most countries are very active in preventing and prosecuting securities fraud and financial market abuse. In part, they do so by requiring that securities be registered and that persons selling them be licensed. Fraudsters often seek to manipulate these perceptions of safety engendered by regulatory systems and to reap the profits that the abuse of securities markets can offer.

3. In addition to the manipulation of the market via insider trading, investors may find themselves subject to high-pressure sales tactics regarding certain securities, or they may fall victim to so-called "pump and dump" schemes that artificially increase the price of the security and the demand for it, thus allowing the fraudster to sell out at the inflated price. Further, funds and assets may be siphoned off by the management of a particular publicly-traded company at the expense of non-controlling shareholders. In general, a high percentage of securities cases involve one or more of these basic violations: unlicensed brokers, unregistered or fictitious securities or fraudulent misrepresentations or omissions, unsuitable recommendations, excessive trading or "churning", market manipulation, or outright theft of funds and assets by corporate insiders.

B. Instances and examples

4. Fraudulent or fictitious securities are promoted in a variety of ways that imitate and expand on the marketing of legitimate securities:

(a) Advertisements or newspaper articles are encouraged or placed containing false or misleading information;

> *Illustration 22-1:* Articles and advertisements were published suggesting that there was a current value for once valid World War I era bonds that had been demonetized by statute and by international treaty.

(b) Unsolicited contacts are made;

> *Illustration 22-2:* Unsolicited phone calls, faxes, letters or e-mails are received from persons presenting themselves as stock promoters

or brokerage firms and advocating that the recipient act immediately on a "hot" tip.

(c) High-pressure sales tactics are used, and there is often an element of urgency connected with the investment;

Illustration 22-3: Promotions suggest that a unique profit opportunity will be lost unless it is acted upon immediately by the investor since only a limited number of people can invest. Allegations may be made that the market is only open for a limited time.

(d) There are assurances of little or no risk;

(e) And often there is reference to so-called "secret markets" in which "trading" occurs.

5. Fraudulent or fictitious securities violate securities laws and regulations and frustrate their scheme of regulation:

(a) The securities are not properly registered;

Illustration 22-4: The fraudster may allege that registration of the securities in this instance is not required;

(b) The person selling the fraudulent or fictitious security often is not licensed as a securities broker;

(c) Or misrepresentations and omissions of material information are made about the profits, risks, and fees associated with investments represented by the securities.

6. Fraudulent securities often are exotic or have exotic features or incredible stories associated with them in order to explain their alleged value.

Illustration 22-5: Metal boxes containing securities allegedly worth billions of United States dollars in so-called "Federal Reserve Notes" were newly discovered in the Philippines after being hidden by an infamous warlord at the end of World War II.

Illustration 22-6: Counterfeit bonds may be created with no value, relying upon an elaborate story involving the loss of Government bonds in an accident.

7. Account statements or transactions statements that have an irregular appearance, suggesting possible forgery to disguise theft.

C. Advice

8. Only deal in securities through reputable channels and brokers.

9. Reject the proposal or contact the appropriate securities regulator to make sure that the salesperson is properly licensed and that the security itself meets applicable registration requirements.

10. Discuss any proposed investment with one's own independent financial adviser prior to investing, particularly when the price of a particular financial instrument seems to be increasing or decreasing rapidly.

11. Review carefully all account statements for signs of irregularities that may suggest a falsified statement intended to disguise theft.

12. Independently verify accounts with the financial house said to hold them.

13. When the security cannot be understood without a complex and convoluted explanation with unusual characteristics, it should be rejected or independently verified.

D. Additional references

Indicator 8. Frustration of due diligence; Indicator 16. Fraud by or involving management and/or employees; Addendum 1. Performing due diligence.

Indicator 23. Misuse of insolvency proceedings

1. The insolvency process can be used as a mechanism to facilitate commercial fraud by facilitating the improper transfer of assets, by obtaining investment in the insolvent entity through misrepresentation, or by filing or selling false claims.

A. Explanation

2. Most legal systems have insolvency legislation to enable companies or individual entities in business to restructure debt through reorganization or liquidation proceedings. Those insolvency regimes provide for substantial oversight in the insolvency process through judicial or administrative supervision if properly used. The insolvency processes serve important commercial and policy needs for businesses experiencing financial difficulties.

3. While frauds may often result in the filing of an insolvency proceeding relating to the victim, fraudulent schemes also use the legal process related to insolvency to mask or facilitate commercial fraud, and to use the credibility of the insolvency process to provide a false sense of security to intended victims. Fraudsters use the insolvency process to misrepresent that the insolvency court or representative has reviewed and approved of representations purportedly made on behalf of the insolvent entity. Fraudsters also can use the insolvency process to hide the improper transfer of assets or to file and sell false claims.

B. Instances and examples

4. The insolvency process can be used to hide assets from existing creditors.

> *Illustration 23-1:* Before entering insolvency, an entity may shift assets from one jurisdiction to another in order to hide the assets or to establish a new business operation. Creditors of the entity are then denied recovery, because the entity has insufficient assets to pay prior debts.

> *Illustration 23-2:* Prior to an entity entering insolvency, the principals of the entity transfer assets to themselves or to other insiders, thus denying available funds to creditors of the entity.

5. The fraudster may misrepresent the value of assets or business enterprises of the insolvent entity.

> *Illustration 23-3:* The fraudster undervalues the assets of an insolvent entity, so that creditors are induced to accept substantially less than full value of the debt owed.

> *Illustration 23-4:* The fraudster may overvalue assets of an insolvent entity, knowing that victims will believe the fraudster's valuations have been reviewed by or verified by the court or insolvency representative. Victims then invest in the insolvent entity, believing that the entity's financial position is better than it is.

6. False claims may be filed in the insolvency proceeding to defraud creditors or potential investors.

> *Illustration 23-5:* Once an entity enters insolvency proceedings, the principals of the entity file false claims, inducing the court and insolvency representative to distribute less to valid creditors as well as portions of the assets to the principals.

> *Illustration 23-6:* A fraudster files false claims against an insolvent entity and sells the claims at a discount to victims who, believing the claims to be valid, attempt to collect from the insolvent entity.

7. The existence of insolvency proceedings may be used to facilitate a fraud.

> *Illustration 23-7:* A fraudster induces a victim to provide the insolvent entity with goods, services or credit. Victim is told that the court or insolvency representative has guaranteed payment or otherwise assured the victim of repayment by giving its authorization or approval, when in fact it has not.

> *Illustration 23-8:* Another fraud can take place when a party knows it is insolvent and enters into a transaction requiring a prepayment, declaring insolvency subsequent to the receipt of the prepayment.

C. Advice

8. Remember that insolvent entities are in insolvency proceedings as a result of being unable to pay existing creditors or of failing in its business enterprise. Any proposed transaction with or investment in the insolvent entity must be carefully reviewed prior to any investment made.

9. Always exercise proper due diligence and independently investigate any representations of value by the insolvent entity before extending any additional credit or providing goods and services on credit.

10. Because insolvency proceedings are generally a matter of public record, the insolvency proceedings should be reviewed to verify any representations supposedly made by an insolvency court or insolvency representative.

11. Never suspend the exercise of due diligence on a mere assertion by a counterparty that an insolvency court or insolvency representative has approved or authorized a transaction or investment.

12. Carefully review any transfers of assets by the insolvent entity both prior to and during the insolvency proceeding to determine if such transfers are legitimate.

D. Additional references

Indicator 8. Frustration of due diligence; Addendum 1. Performing due diligence.

Addendum 1. Performing due diligence

The appropriate performance of due diligence will depend upon the particular circumstances of the transaction in issue, but it is possible to articulate some general rules that should be followed in ascertaining the bona fides of a transaction and of counterparties. Remember that this list contains only general guidance, and that other sources should be considered for more detailed assistance, for example, the website of the Anti-Phishing Working Group (www.apwg.com); the website of the United States Federal Trade Commission (www.ftc.gov); the website of an international consortium of consumer protection agencies, Consumer Sentinel (www.consumer.gov); another international consortium, Econsumer (www.econsumer.gov); or the European Union consumer website (http://ec.europa.eu/consumers/index_en.htm).

A. Determining how one was chosen for contact

1. If the investor did not initiate the contact, inquire as to how the counterparty obtained one's name and contact information.

2. Inquire as to why the counterparty is contacting the particular investor. Why does the counterparty think the investor is appropriate for a business transaction? Vague or general answers indicate that the counterparty does not have a good basis for determining one's suitability for the transaction.

B. Verifying the counterparty

3. Always seek contact numbers, information and the identity of the counterparty and its representatives independently of the information provided by the promoter of the investment, via Internet, telephone books, business organizations, the press, library materials or the like. Do not rely on telephone numbers, websites, addresses or the views of professionals provided by the promoter of the investment in performing due diligence.

4. When dealing with a professional, ascertain from the relevant professional organization whether the professional is properly registered and qualified by the organizations and the history of the professional, including any complaints made or charges brought against that professional.

5. If possible, check the names of counterparties and promoters for criminal history or complaints with criminal fraud authorities in one's jurisdiction. Remember that aliases may be used by fraudsters.

6. Remember that fraudsters may work in teams, and corroboration by other people, particularly those suggested by the promoter, may not be sufficient to protect oneself.

C. Recognizing sales tactics

High pressure

7. Do not abandon the completion of thorough due diligence when faced with emotional appeals, such as those purporting to involve humanitarian crises.

8. Do not succumb to time pressures such as the need to invest or purchase immediately because the opportunity is about to be lost. If the deal is that good, the promoter would not need to contact individual investors. If one is discouraged from conducting due diligence due to time pressures, do not proceed with the transaction.

Expectations

9. Check the key facts of the transaction, including predictions of rates of return, against current economic events, such as the price or amount of a particular commodity in issue, or the normal trading patterns of the commodity.

D. Identifying the product

10. Determine the product that is being sold. Sometimes the product is a service or an intangible legal right disguised as a physical product.

11. Intangible rights such as options to buy, time share arrangements, rights to lease and the like are very difficult to verify as to their existence. Extra due diligence will be necessary to verify their authenticity.

12. Products that are stored in a different local jurisdiction or overseas are easily falsified and will also need additional due diligence.

E. Identifying the nature of the transaction

13. Determine what one is being asked to do: make a down payment, pay a finder's fee, enter into a "swap" transaction, set up an escrow, purchase a letter of credit or similar events that are only part of the transaction. Many of these transactions do not transfer any property rights to the customer, but are preliminary at best.

14. Consider using a trusted broker as a "middleman" to hold funds pending contract performance or delivery of goods.

15. Verify that any funds sent are returnable if the transaction does not complete.

F. Determining the mechanics and documentation of the transaction

How funds are handled

16. Determine where funds are being sent for payment and verify the recipient institution. Is it a reputable financial institution in a reputable jurisdiction or is it an offshore account? Legal remedies in offshore centres are generally weak for individual investors.

17. If the money is being held in escrow or in a letter of credit, is the financial institution in good standing and with a good reputation?

18. Verify signatures, accounts and other documentary information provided by contacting, for example, the organization on whose letterhead the information is printed, or the person who has purportedly signed the document.

19. Any security vehicles or documents provided, such as letters of credit, guarantees, or the like, should be verified by calling the other parties mentioned in the document to ascertain their validity.

How to communicate with the counterparty

20. The counterparty should be easily accessible by phone, mail or e-mail. The information should be independently verifiable.

21. Personal visits to the counterparty's offices should be available to get an idea as to the nature of the counterparty. Care should be taken as appearances may be deceiving.

What information is exchanged with counterparty

22. Care should be taken as to what information is given to the counterparty. Business information is appropriate but personal information is not in a normal commercial transaction.

23. Personal information should only be given to financial institutions such as securities and commodities brokers after verifying their registration and good standing with the relevant regulatory authorities.

G. Researching the parties, products and transactions

24. Increasingly, materials on ongoing fraudulent schemes and warnings regarding domestic or foreign fraud areas are being publicized by regulatory

authorities and business and consumer organizations. Efforts should be made to locate such materials either online or via local business organizations.

25. Follow up on any uneasiness one may have, for example, a telephone area code that does not fit the purported location, or facts that do not make sense.

26. Engage in some comparison shopping for similar products or transactions, if possible.

27. If dealing with products, try to obtain a sample to have it analysed, or try to have the item in question appraised by a qualified and independent party.

28. Start one's inquiry on a regional basis, looking to domestic private and governmental organizations for information, then broaden the approach to encompass cross-border review, into jurisdictions referred to in the documentation or by the promoter as well as those that have not been mentioned, which may have been the site of previous frauds.

29. If a very large investment is being considered, hire the services of professionals to conduct due diligence on the promoter and the proposal.

30. Even if the relationship is an ongoing one, treat every new investment or significant transaction with the same caution and the same approach to due diligence.

United Nations publication
Printed in Austria

V.13-85552—September 2013