United Nations A/CN.9/624/Add.2

General Assembly

Distr.: General
10 May 2007

Original: English

United Nations Commission on International Trade Law
Fortieth session
Vienna, 25 June-12 July 2007

Indicators of Commercial Fraud

Note by the Secretariat*

Contents

* This note is submitted late due to the need to complete consultations and finalize subsequent amendments.

V.07-83566 (E) 160507 170507

Indicator 16: Fraud By or Involving Employees

Employees (or other corporate insiders with access to similar information or systems, including 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.

Explanation:

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 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.

Instances and Examples:

- 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 has access to valuable documents, steals and sells them.

- 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.

- 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.

- 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 like 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.

- 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.

- The work of a senior employee 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.

Advice:

- Entities should use independent auditing committees, analytical review and surprise audits of both successful and unsuccessful aspects of operations.
- Employers should create fraud and conflict of interest policies and should ensure that employees are informed of them and trained in their operation.
- Employers should have effective whistleblower policies in place, and ensure that employees are informed of them and have confidence in their operation.
- Employers should ensure that all employees and senior managers are adequately supervised.

- Employers should perform periodic reviews of company contracts and agreements to eliminate contract and procurement fraud, such as kickbacks, bribery and conflicts of interest.
- 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.
- 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.
- Employers should create periodic job rotation, provided it is consistent with local labour laws.
- 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.
- Employers should consider programmes to encourage loyalty amongst employees, including paying them competitive salaries.
- Employers should be alert for sudden changes in an employees' lifestyle, including extravagant purchases or excessive lines of credit.
- Employers should ensure that the knowledge and skill of employees are consistent with the position they hold.
- Employers should check references or credentials in employment applications or resumes.
- In general, employers must create a robust control environment in the business in order to prevent fraud.

See also: Indicator 8 – Frustration of Due Diligence; Indicator 9 – Corrupted Incentives; Addendum 1 – Performing Due Diligence.

Indicator 17: Unusual Involvement or Participation of Professionals

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

Explanation:

Commercial transactions naturally involve professionals in a variety of roles. Moreover, businesses rely on professionals for advice and to protect them 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.

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.

Instances and Examples:

- 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.

- 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.

- 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. 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.

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

  Illustration 17-5: An independent lawyer or an accountant is engaged to assist on the transaction, but is provided with false financial statements and accounting records.

Advice:

- 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.
- Never suspend due diligence solely because a counterparty's professional advisor claims to have found the transaction to be legitimate.
- 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.
- 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.
- Professionals should question unusual instructions received from their clients.
- 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.
- 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.

See also: Indicator 1 – Irregular Documents; Indicator 4 – Misuse of Names; Indicator 8 – Frustration of Due Diligence; Indicator 10 – Ensnarement and Psychological Inducements; Addendum 1 – Performing Due Diligence.

Indicator 18: Inappropriate Requests for Information Disclosure

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.

Explanation:

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.

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.

Instances and Examples:

- 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 spyware) may be used to record and sift every keystroke made on personal computers.

  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.

- 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.

- 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.

- 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.

Advice:

- 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.
- Where appropriate to protect confidential information, employees should be requested to sign confidentiality agreements to protect highly sensitive information.
- Any unusual requests for information should be carefully considered before an entity or individual complies.
- 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.
- 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.
- 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.

See also: Indicator 8 – Frustration of Due Diligence; Indicator 19 – Unsolicited E-mail and Related Misuse of Technology; Addendum 1 – Performing Due Diligence.

Indicator 19: Unsolicited E-mail and Related Misuse of Technology

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.

Explanation:

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. As one example, many companies seek to expand domestic and international markets by advertising their products or services for sale via the Internet, thereby attracting online attacks against the company, its systems and its customers.

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.

Instances and Examples:

- 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 is used to carry out additional frauds.

- 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 diesel generators 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 generators are 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.

- 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.

- 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 already 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.

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

Illustration 19-6: Fraudsters worldwide use Internet "pharming", that is 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.

- 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.

Advice:

- 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.
- 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.
- 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.
- 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.
- 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.

See also: 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

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.

Explanation:

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.

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

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. Trans-national 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.

Instances and Examples:

- 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. The prospective distributor must purchase a specified amount of merchandise that it may re-sell to its salesman.

  Illustration 20-2: Marketing various products, a company offered prospective distributors direct and override commissions for recruiting salespersons under its supervision. The prospective distributor must agree to purchase a large quantity of goods, which may be resold to its salesmen. 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.

- 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 percent 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-cantered 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 percent per month within three months and 62,500 percent 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 percent returns in exchange for the right to breed insects for medicinal purposes.

- 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.

Advice:

- 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.
- 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.
- 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.
- 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.

See also: Indicator 5 – Disproportionate Returns; Indicator 8 – Frustration of Due Diligence; Indicator 9 – Corrupted Incentives; Indicator 13 – Questionable or Unknown Source of Repayment; Indicator 15 – Fraud Based on Abuse of Personal Affinity or Relationships; Indicator 19 – Unsolicited E-mail and Related Misuse of Technology; Addendum 1 – Performing Due Diligence.

Indicator 21: Frauds Involving Goods and Services

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

Explanation:

Sales of goods 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 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.

Instances and Examples:

- 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, antiquities 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 whiskey.

  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.

- 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.

- 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.

Advice:

- Before entering a transaction relying on the existence of goods, always ensure that the goods exist as represented.
- Never blindly rely on the self-professed expertise of the promoter of the product, particularly when dealing with goods outside one's personal expertise.
- If products are available for inspection, examine carefully the labelling and quality, or where necessary, have the products examined by a reputable expert.
- When the commodity offered is significantly below its wholesale price, be suspicious: obtain a random sample and have it analyzed or appraised by a reputable expert.
- Know one's counterparty, including performing any due diligence necessary to establish the reliability of the counterparty.

- If products are available for inspection, examine carefully the labelling and quality.

See also: Indicator 3 – Inconsistencies in the Transaction; Indicator 8 – Frustration of Due Diligence; Indicator 19 – Unsolicited E-mail and Related Misuse of Technology; Addendum 1 – Performing Due Diligence.

Indicator 22: Securities Fraud and Market Abuse

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

Explanation:

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.

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.

Instances and Examples:

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

  - 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.

- 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.

- There are assurances of little or no risk;

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

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

- The securities are not properly registered;

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

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

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

• 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 US 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.

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

Advice:

• Only deal in securities through reputable channels and brokers.

• 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.

• 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.

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

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

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

See also: Indicator 8 – Frustration of Due Diligence; Addendum 1 – Performing Due Diligence.

Indicator 23: Misuse of Insolvency Proceedings

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.

Explanation:

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.

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. Finally, the insolvency process can be used to provide credibility for the insolvent entity, so that it may obtain additional goods, services, or credit.

Instances and Examples:

- 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.

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

  Illustration 23-3: 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: 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.

- 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, attempts to collect from the insolvent entity.

- The insolvency proceedings may be used to lend credibility to the insolvent entity.

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 transaction requires a prepayment, and the other party claims that it is insolvent subsequent to the receipt of the prepayment.

Advice:

- 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.
- 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.
- 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.
- 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.
- 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.

See also: 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 US 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).

1. Determining how one was chosen for contact

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

2. Verifying the counterparty

- 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.
- 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.
- 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.
- 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.

3. Recognizing sales tactics

High pressure

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

- 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.

4. Identifying the product

- Determine the product that is being sold. Sometimes the product is a service or an intangible legal right disguised as a physical product.
- 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
- Products that are stored in a different local jurisdiction or overseas are easily falsified and will also need additional due diligence.

5. Identifying the nature of the transaction

- 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.
- Consider using a trusted broker as a "middleman" to hold funds pending contract performance or delivery of goods.
- Verify that any funds sent are returnable if the transaction does not complete.

6. Determining the mechanics and documentation of the transaction

How funds are handled

- 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.
- 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?
- 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.
- 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

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

- 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 that appearances are deceiving.

What information is exchanged with counterparty

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

8. Researching the parties, products and transactions

- Increasingly, materials on on-going 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 on-line or via local business organizations.
- 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.
- Engage in some comparison shopping for similar products or transactions, if possible.
- If dealing with products, try to obtain a sample to have it analyzed, or try to have the item in question appraised by a qualified and independent party.
- 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.
- If a very large investment is being considered, hire the services of professionals to conduct due diligence on the promoter and the proposal.
- 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.