Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Glossary of Fraud Schemes and Terms

David McNamee, CIA, CISA, CFE
Contact Telephone: 1-925-934-3847

Abuse: In some cultures, a minor *Fraud* or infraction.
Accomplice: In fraud, a partner to the fraud scheme. See also *Perpetrator* and *Shill.*
Advance Fee Scheme: The *Fraudster* collects fees in advance without ever intending to fulfill the agreement to provide services or products.
Affidavit: A sworn statement.
Affiliate Bidding: A condition in purchasing when multiple bids are tendered for a contract from a single company under various names to give the appearance of competition.
Agent: A person with an agency relationship (employee or independent contractor).
"At will": An employment situation where the employee is not protected from arbitrary firing -- the employee works only at the pleasure of management and may be terminated at any time for no reason. Contrast *"For cause."*
Backdate: To post a date on a document earlier than the actual creation date for purposes of deception.
Back Door: In computer fraud, unauthorized entry point or weakness discovered by a *Hacker*. Similar to *Trapdoor*, except that back doors are usually pre-existing weaknesses.
Bait and Switch: In consumer fraud, advertising a low cost item and then steering the customer to a higher priced item when they come to buy, claiming the low priced item was "sold out."
Bank Examiner Scheme: The *Fraudster* poses as a Bank Examiner who is trying to catch a dishonest teller. The Bank Examiner needs the victim to withdraw a substantial sum from their account to test the teller. The Bank Examiner then asks the victim to hand over the cash for a receipt while they use the cash as evidence. The fraudulent Bank Examiner then disappears with the cash, and the receipt turns out to be worthless.
Bankruptcy Fraud: The *Perpetrator* files a notice of bankruptcy. He then approaches each of his creditors (who have received a cop of the notice of bankruptcy) and tells each one in turn that they are the special one that he wants to see get paid at least something. The creditor often settles for 10% of the amount owed. Once a settlement with one creditor is reached, the Perpetrator approaches the next creditor, and so on until all creditors have been settled with at a small fraction of the outstanding amounts owed. The Perpetrator then withdraws his petition for bankruptcy, have extinguished most of his debt for a small fraction of the original amount.
Bid Rigging: In purchasing, any scheme that gives the appearance of competitive bids but is actually not competitive because the participants establish

the winner before submitting bids for the contract. See *Affiliate Bidding* and *Bid Rotation*.

Bid Rotation: In purchasing when bidders for contracts *Collude* to distribute work among themselves by establishing which among them will win particular bids.

Boiler Room Operation: A fraud scheme that attempts to sell worthless securities (or similar assets) over the telephone through high-pressure sales tactics. If the money is sent in or the credit card number given out, there is nothing of value received.

Bribery: To offer money in exchange for favourite treatment or to compel or influence some action. Official (government employee or elected official) bribery involves a promise for acting or withholding some official act. Official bribery *(Corruption)* is unlawful in most cultures. *Commercial Bribery* is known as "facilitating payments" in some cultures and is not a crime in most cultures, although it often is against the organization's policies and procedures.

Bucket Shop: A securities fraud scheme that pretends to buy and sell securities for customers, but actually never invests the money it receives. The scheme depends upon stock price manipulation or a continuously rising market to encourage more buyers than sellers. Also associated sometimes with the *Pump-and-Dump* scheme.

Case Method: In fraud *Investigation*, a six-step process of gathering evidence in order to identify a Suspect.

Chain of Custody: In evidentiary matters, the record of possession from original discovery until produced at trial. If the chain of custody is broken or unclear, the *Evidence* may be challenged as not the original or not in its original condition.

Chain Letter Schemes: Letters with names listed and claims that the recipient of the letter, by putting their name on the list, removing the top name and sending them some nominal amount, then mailing the new list to some number of friends and acquaintances, will receive a lot of riches in the mail. There is usually also a "curse" or bad luck associated with individuals who "break the chain."

Check Kiting: See *Kiting*.

Code of Conduct: See *Code of Ethics*.

Code of Ethics: A document adopted by an organization that describes the expectations of the organization of employee and management behaviour to all employees, suppliers, customers, the government, and the community.

Coerce: To influence action against someone's will, usually by threat.

Collateral Frauds: Fraudulent representing collateral for loans that (1) does not exist, (2) is not owned by the loan applicant, or (3) is grossly over-valued, or some or all of these.

Collude: In the context of *Fraud*, to act together for a fraudulent purpose.

Commercial Bribery: Giving and accepting payments to favour or not favour a commercial transaction or relationship. See also *Bribery* and *Corruption*.

Computer Virus: See *Virus*.

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Con: Short form of *Confidence Game.*
Conceal(ment): The second step in committing a Fraud. To hide from view.
Confidence Game: A fraud scheme where the *Perpetrator* gains the confidence of the *Mark* to defraud the Mark in some way. Perfect Confidence Games are so effective that Marks do not report them to the authorities for fear of looking foolish or because the game involved something unlawful (such as illegal gambling).
Conflict of Interest: An employee owes a duty to the employer to act in the interest of the employer (and no other) when carrying out the duties of an employer. A Conflict of Interest exists when the employee has some personal kinship, friendship or financial interest in the transaction that may divide the employee's interests and put his duty to his employer in jeopardy.
Conspiracy: Two or more persons come together for the purpose of committing a *Fraud*.
Conversion: The third step in a *Fraud*. To exchange for personal gain.
"Cooking the Books": Altering the official accounts to deceive. See also *Journal Entry Fraud.*
Corruption: *Bribery* of a government official. See also *Commercial Bribery.*
Cost of Goods Sold changes: Unusual changes in cost of goods sold, as a percentage of sales may be an indicator of the theft of revenue or theft of finished goods inventory. See *Fictitious Refunds Fraud*.
Covert: Hidden or secret, as in *Covert Operations*.
Covert Operation: A plan or activity to obtain evidence through *Operatives* or *Agents* whose true role is undisclosed to the target. Examples of covert operations include *undercover* work and *Pretence*. See also *Ruse*.
Cyber-crime: Referring to frauds perpetrated on the Internet or through the use of computers.
Cycle Counts: In inventory control, counting various portions of the inventory frequently until it is all counted (vs. counting the whole inventory once a quarter or once a year).
Defalcation: A fancy word for *Fraud*, theft or other dishonest act relating to a position of trust in an organization.
Defamation: The act of knowingly uttering *Slander* or printing *Libel* that is untrue but harms another person's character and reputation.
Denial of Access attack: A computer *Virus* or computer program run to generate many thousands of requests to the central computer, thereby tying up the processor and denying legitimate requests of access.
Deposition: A pre-trial legal proceeding in which a person is questioned under oath by an attorney, usually witnessed and recorded by audio, video, and/or written verbatim notes. The purpose of the deposition is to discover *Evidence* that may be used later at trial or to induce the person to make statements of knowledge or fact that can be used at trial.

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Directory Advertising Schemes: Fraudulent invoices claiming that the company is listed in a business directory and requesting payment. There may or may not be such a directory, and the directory may or may not ever be distributed or distributed as widely as claimed. For certain, no one ever ordered or authorized the directory advertisement. See also *Shipping Short.*

Direct Inward System Access: A feature on PBX (Private Branch Exchange) telephone equipment that is vulnerable to fraud. It is used to allow people outside of the office to call anywhere in the world through the *DISA* port using a toll-free number and a *PIN* (Personal Identification Number). *Hackers* attack the PBX through the toll-free number and try to break in by guessing the PIN. If successful, the hackers can use the telephone network of the victim to place calls billed back to the victim.

DISA: See *Direct Inward System Access*.

Documentary Evidence: Written or photographic representations of fact.

Dual Custody: A method of protecting cash by requiring all cash assets handled by two people (two signatures, two keys, two people counting, etc.).

Dummy: Fictitious.

"Dumpster Diving": Rummaging through someone's trash to obtain information.

Eavesdropping: See *Electronic Surveillance*.

Electronic Surveillance: Listening and/or recording activities using electronic means (audio and video) without being detected. In some jurisdictions, electronic surveillance is unlawful without permission from all parties.

Embezzlement: Theft of money from an employer by an employee using false entries in accounting records to cover up the crime. See also *Journal Entry Fraud.*

Employee Account Fraud: When employees are also customers, employees may make unauthorized adjustments to their accounts (including write-off).

Entrapment: Unlawfully lured into a crime by a police officer. A common defence in a criminal activity where the criminal claims they were innocent and would not have been involved in the crime otherwise.

Expense Report Fraud: Charging unauthorized or fictitious amounts on an expense report. See *Padding Expense Accounts*.

Exposure: The potential for loss.

Extortion: The offer to keep from harm in exchange for money or other consideration. The demand for *Restitution* in exchange for not prosecuting a crime is a form of extortion.

Factors of Fraud: Opportunity (an opening or control weakness to be able to commit the fraud), Pressure (a problem that cannot be shared or resolved), and Attitude (a propensity to steal or the ability to rationalize fraudulent behaviour). All frauds have these three factors as a cause.

False Claims: Claims for reimbursement by an employee or contractor for nonexistent or inflated expenses. False claims can be for business expenses or personal expenses (such as medical). See *Padding Expense Accounts*.

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

False Credentials: Misrepresenting education or experience or professional certification to fraudulently obtain and hold employment.
False Imprisonment: During an *Interrogation*, blocking the subject's avenue of escape, essentially holding the person against their will. Unless the person has been arrested, they may not be detained against their will at any time.
False Pretence: See *Pretence, Ruse* or *Subterfuge*.
Fictitious Refunds Scheme: Preparing false documents of refunds to cover thefts of cash. A retail cashiering fraud. See *Cost of Goods Sold changes.*
Fictitious Sales: A scheme to record sales to fictitious customers or fictitious sales to existing customers at the end of one period and reversing the transactions at the beginning of the next period. The purpose of the scheme is to inflate sales to create false profit statements or earn unwarranted bonuses. Excessive credit memos or sales cancellations at the beginning of an accounting period can be an indicator of this fraud.
Fiduciary Duty: The acts necessary (usually of an authorized employee or agent) to carry out a responsibility to care for assets prudently. See *Embezzlement*.
Firewall: A software program that protects direct access to a local area network by establishing a "public" network in front of the "trusted" network. The purpose of the program is to secure data and systems from *Hackers*.
"For cause": An employment arrangement where employees may only be terminated for a proven cause. For contrast, see *"At will."*
Forensic: Suitable for use in a court proceeding.
Forensic Auditing: Examination of a business process for evidence of *Fraud*.
Forgery: Creation of false documents or altering existing documents, especially financial instruments or other authorizations.
Fraud: A theft, concealment and conversion to personal gain of another's money, physical assets, information, or time.
Fraud Scenarios: A method of developing mental models of possible *Frauds*. "Thinking like a crook."
Fraudster: One who commits the *Fraud*.
"Ghost" employees: Fictitious employees on the payroll, for whom the supervisor or manager receives the extra paychecks.
Hacker: (Old) one who enjoys unravelling the mysteries of the computer. (Modern) A person who attacks another's computer and seeks to gain unauthorized access by hacking (breaking down) the computer's logical security.
Hearsay: they not personally and directly know a weak form of evidence that is an opinion of the witness or that.
Hidden Bank Accounts: A possible indication of *Embezzlement, Bribery* or *Kickback* frauds.
Hot Line: A telephone number to report suspected Fraud. Often hot lines are handled as anonymous tips.
Impeach: In *Testimony*, to catch the person in a lie or contradiction of fact.

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Improprieties: A polite word for *Frauds* and wrongdoings.
Inflated Inventory: An indication of *Embezzlement* or possible theft of inventory. See *Inventory Shrinkage*.
Influence Pedaling: The offer by a government official to use their office to influence actions for a private party in return for something of value.
Informant: A person, such as a co-worker or friend of the accused, used in the investigation of a fraud that may know something about the crime but is otherwise not involved.
Insider Trading: Using business information not released to the public to reap profits trading in the financial markets.
Interrogation: An interview of a suspect conducted for the main purpose of obtaining an admission of guilt, to identify and neutralize defences the target may raise, and to obtain information used to impeach the *Suspect*.
Interview: A structured (planned) question and answer session with a person designed to elicit information.
Inventory Shrinkage: Theft of physical inventory.
Investigation: A structured gathering of *Documentary Evidence* and *Testimony* to solve a reported *Fraud*.
Irregularity: A polite word for *Fraud*.
Journal Entry Fraud: Using accounting journal entries to fraudulently adjust financial statements. See also *Embezzlement*.
Kickback: A payment by a vendor to an employee at the request of the employee in order for the vendor to receive favourable treatment.
Kiting: Using several bank accounts in different banks, making deposits and writing checks against the accounts before the deposit checks clear the banking system, creating a "float" of money out of nothing more than the lag in time while checks clear and post to their respective accounts.
Lapping: Stealing a customer payment and then using a subsequent customer payment to cover the previous customer's account. This overlapping payments creates a "float" of money that can be used as long as all payments are eventually posted. What usually occurs is that the lapping process builds up like a giant pyramid until it falls apart when not enough payments are available to cover the amounts owed.
Libel: Knowingly publishing false statements about another person that creates harm.
Lie Detector: See *Polygraph*.
Lifestyle changes: A possible indicator of theft is the sudden change in lifestyle such as exhibiting more than usual wealth.
"Lowballing": Placing an unusually low bid to win the business. Often with the intent to inflate the price later with extras or change orders. Also can indicate a defective *Request for Proposal.*

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Maintenance Port: An access point in the PBX (Private Branch Exchange) telephone equipment that is vulnerable to fraud. The port exists to allow the manufacturer's repair technicians to call into the PBX from a remote location and diagnose problems or administer maintenance software patches. Also known as the *Remote Access Unit*, or *RAU*.
Malicious Prosecution: Targeting someone for prosecution without reasonable grounds for suspicion.
Mark: The intended victim of a *Swindle* or *Confidence Game*.
Misappropriation: A polite word for theft.
MLM: See *Multi-Level Marketing.*
Moving Surveillance: Following the target of surveillance from one position to another, as in *Shadowing* or *Tailing* a suspect.
Multi-Level Marketing: A form of *Pyramid Scheme*, not necessarily fraudulent, where sales are made to retail customers and commissions earned through many levels of the chain within the pyramid. The chain is built and expanded by each layer constantly recruiting more people to sell the product or service.
Negative Invoicing: Using an invoice for a negative amount to cover a theft of a customer payment. The negative invoice is less noticeable than a credit memorandum and usually under less stringent control. A negative invoice is a symptom of possible theft.
Nigerian Letter: A fraud scheme that now includes faxes and email versions of a letter from a supposed official in Nigeria. The official has a large sum of money (often stated as $20 to $30 million) to transfer out of the country. Due to exchange controls, the official asks for the victim's help with the transfer. All that is required to earn a hefty reward/commission is to furnish the Nigerian official with your bank account number, and they will handle the rest. What actually happens is that the *Perpetrator* depletes the victim's account.
Obstruction of Justice: Impeding a lawful Investigation by such acts as providing false documents, false testimony, destruction of evidence, and intimidating witnesses.
Ombudsman: A person who acts as an advocate for employee grievances against the organization. Also, a neutral party to whom employees can turn to report *Fraud*.
Operative: A person acting on your behalf or under your care, custody or control in a specific manner. A source or *Informant* working *Undercover* in *Covert Operations* is an operative. There is no agency relationship with an operative as with an *Agent*.
Over billing schemes: Padding invoices with extraneous or fictitious items. Intentional duplicate billing, such as billing two parties for the same work is also an over billing scheme.
Overt: Open, not hidden. See *Covert* for contrast.

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Out-of-Route: Outside sales or service workers who deviate from their normal route or time schedule, such as conducting personal errands or taking excessively long coffee or lunch breaks.
Outstanding Items: In checking operations, checks that have been written but not cleared through the bank. An equivalent banking term for interbank transactions.
Padding Expense Accounts: Adding extra expense items or inflating the value of legitimate expense items to obtain unwarranted reimbursements.
Padding Overtime: Adding extra hours to falsely inflate the payroll and earn unwarranted pay.
Palming: To conceal in the hand.
Perjury: Lying under oath, including sworn court appearances, *Depositions*, *Affidavits*, and other sworn statements and documents.
Perpetrator: The person who commits the *Fraud*.
Personal Identification Number: A code used to access personal data or accounts.
Pilfering: *Theft*, usually referring to theft of physical goods. In retail business, customer theft is known as *Shoplifting* and employee theft is called pilfering. Occasionally used also with theft of cash, especially petty cash or for small thefts.
PIN: See *Personal Identification Number*.
Pigeon Drop: A fraud scheme that involves a wallet/purse/envelope with a large sum of money in it but no identification. The *Perpetrator* and *Accomplice*, together with the victim "finds" the wallet, and the victim is persuaded to withdraw a sum of money as "good faith" to share in the cache. The victim is distracted and the Perpetrators steal the money and disappear with it.
"Pingponging": In medical insurance or *Workers Compensation Fraud*, referring patients to other doctors in the same clinic in order to claim reimbursement for "consultations" rather than for actual treatment. See also *False Claims*.
Polygraph: A machine for recording a number of life signs (breathing rate, pulse, etc.) to aid in determining if a *Suspect* is lying. Also known as a *Lie Detector*.
Ponzi Scheme: A fraud in which a high rate of return is promised on investments. The first few investors receive the high rate of return from part of the investments of later victims. At no time is any actual investment made.
Pretense: Also *False Pretense*. To represent something to be what it is not. See *Ruse* and *Subterfuge*.
"Pump-and-Dump": Manipulating stock prices by artificially creating demand through rumour, high-pressure sales tactics, or multiple large orders. The price is "pumped" upwards and then when other investors join the trend, the original investors "dump" the stock in a rapid sell-off. See also *Bucket Shop.*

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Pyramid Scheme: A commercial version of the *Chain Letter* scheme where the *Fraudster* sells bogus distributorships, franchises or business opportunity plans to people who are in turn induced to do the same. See also *Multi-Level Marketing*.
"Razoring": Removing the last check, invoice, purchase order or other sequentially numbered item from a pad of items by carefully cutting with a razor around the staple holding the pad together. In this manner, fictitious transactions can be documented on official forms.
RAU: *Remote Access Unit.* Also known as the *Maintenance Port*.
Reconciliation: A process of comparing details with control totals, such as checks paid during the month and deposits made that month with the change in bank balance at end of the month.
Red Flags: Symptoms and indicators (of *Fraud*).
Remote Access Unit: See *Maintenance Port*.
Request for Proposal: A request to potential vendors for tender offers or bids to perform a service or provide a product (or both) to solve a particular business problem. See also *Request for Quote.*
Request for Quote: A request to potential vendors for price quotes and delivery terms -- usually for much simpler procurement requirements than *Request for Proposals*.
Restitution: Restoring money or property to the victim of a *Fraud*.
Resume Inflation: See *False Credentials*.
RFP: See *Request for Proposal*.
RFQ: See *Request for Quote.*
Rube: A slang term for a *Mark* or victim, especially someone who appears naïve.
Ruse: A scheme that tries to make something appear as something else. Hiding the true meaning or acting out a lie. A *Subterfuge* or *Pretense*.
Sabotage: Destroying or delaying some part of the business process.
"Salami": In banking, a fraud that involves taking all of the "round-down" fractional cents from periodic interest payments and crediting them to a single account. Thus each transaction has only a thin slice removed.
"Salting" cash: Testing accounts receivable employee honesty by placing some cash in the customer receivables process to see if it is reported as cash or stolen.
Secure Socket Layer: A protocol used in electronic commerce to afford more security to transactions on the Internet.
Self-approval: The act of authorizing a transaction for one's own benefits or gains, or an act of approval for an activity in which the approval authority participated.

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Sewer Service: Many consumer frauds rely on litigation to win judgments to collect the proceeds of the fraud. These organizations limit the ability of the victim to defend against this litigation by not informing them of the suit (literally dropping the *Subpoena* "down the sewer") and filing false *Affidavits* in court that the litigation papers had been properly served.
Shadowing: Following the suspect or target of *Surveillance* from place to place to observe activities without being detected.
Shell Game: A game where a pebble or dried pea is hidden under one of three shells or cans. The *Perpetrator* moves the shells around quickly, often *palming* the pebble, and then asks the *Mark* to choose the shell where the pea is located. A common street *Confidence Game*. See also *Sleight-of-hand*.
Shill: An person in a *Confidence Game* that acts as a participant to draw in the *Mark*. An *Accomplice* -- one who is paid to play as part of a *Swindle*. Derived from casino gambling, where the shill is a paid employee used to attract other gamblers.
Shoplifting: Customer theft from retail inventory. See also *Pilfering*.
"Short-and-Over": An account used in cashiering operations to track the imbalance of cash to sales recorded. A perfectly balanced cash operation day-after-day, with no shorts or overs, is a symptom of possible theft. It is unusual to never make mistakes handling money.
Shorting: In medical frauds, delivering less prescription medicine than actually charged to the insurance company or government.
Short Shipping: Shipping less than the quantity shown on the invoice (or shipping nothing at all; see *Directory Advertising Scheme*).
"Shoulder Surfing": Observing someone using a *PIN* (*Personal Identification Number*) by covertly looking over their shoulder, sometimes with the aid of binoculars or video camera with zoom lens.
Shrinkage: See *Inventory Shrinkage*.
Slander: Knowingly uttering false statements about another person that causes harm.
Sleight-of-hand: A magician's trick. The ability to conceal a physical action by distracting the participant. See also *Palming*.
Spying: See *Surveillance*.
SSL: See *Secure Socket Layer*.
Stakeout: See *Stationary Surveillance.*
Stationary Surveillance: Observation of activities of a suspect from one vantage point. Also known as a *Stakeout*.
Statutory Employee: An employee by action and tax law, but not actually on the payroll. There are potential violations of USA tax and employment benefits laws if independent contractors and consultants are found to be statutory employees instead.
Suborn: The act of *Bribery*.
Subterfuge: Masking the true nature or reason for an action.

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Surveillance: Gathering evidence through observation from outside of the operation (contrasted with Undercover). Surveillance can be *Moving Surveillance, Stationary Surveillance* or *Electronic Surveillance*. Also known as *Spying* or *Eavesdropping*.
Suspect (n.): The target of the fraud Investigation. See also *Perpetrator* and *Fraudster*.
Suspect (v.): To place under suspicion of wrongdoing.
Swindle: A scheme to obtain money by *Ruse* or *False Pretense*. See also *Confidence Game*.
Tailing: See *Shadowing.*
Testimony: Oral evidence (representations of fact) taken by *Interview* or *Interrogation*. Testimonial evidence is necessarily weaker than *Documentary Evidence*.
Theft: The first step in a *Fraud*. Unlawfully taking.
"Thief's Calculator": A collection of innocent-looking bits and pieces near the cash register for the purpose of tracking the amount of cash stolen by *Skimming*.
"Tone at the Top": The messages and actions of senior management in relation to *Fraud* detection and deterrence.
Trapdoor: In computer fraud, a means of unauthorized access to the computer operating system or files, usually placed by a *Hacker*.
Trojan Horse: A type of computer program that remains inert (and possibly hidden) until activated by an external event such as a date. Used as *Viruses* to disrupt or destroy computer operations, or used to open a *Trapdoor* for unauthorized access.
Unauthorized Use: Policies should be in place to determine what business resources may be used for personal business and at what times. Other use constitutes *Theft*.
Undercover: Secret or *Covert Operations* where a person works under an assumed identity, adopts a disguise, or takes on an assumed role in order to gather evidence.
Under-ring: To record less than the actual sales price. Usually refers to a cashier ringing a sale on a cash register. Under-rings may be a method used in *Skimming* cash by the cashier, or they may be used to give unauthorized discounts to an Accomplice.
Unethical: Behaviour that does not meet community standards for "right behaviour," but that does not violate any laws either.
Unlawful: Behaviour that violates established laws.
Virus: In computer operations, a program that is deliberately released to a system with the ability to replicate itself and spread by attaching unauthorized data to files. Viruses can be benign, just taking up disk storage space, or they may be vicious and actually destroy data or deny authorized access.
Voids: In cashiering, ringing a "Void" to cancel a previous sale. Excessive voids may be a sign of theft.

Heads Up Fraud Prevention Association
9620 – 103A Avenue Edmonton, Alberta T5H 0H7
Toll Free: 1.877.877.4323 Fax: 780.439.5717 Email: info@heads-up.ca
Web Site: www.heads-up.ca

Whistle blowing: The act of an employee revealing suspected fraud (usually involving senior management) to an outside third party.
Witnesses: People who may have information of a *Fraud* based on observation.
Worker's Compensation Fraud: False claims for on-the-job injuries. Usually takes the Collusion of employee and unscrupulous doctors to submit false diagnoses. Back injuries (soft tissue strains) and stress are the most common ailments used in this scheme.