Recognizing, Avoiding, And Reporting Frauds In Business World

Fraud comes in many different shapes and sizes. Fraud affects everyone regardless of their skin color or the language that they speak. There are several types of fraud in international trade. Criminals can tap into your business bank account, hack your website, make phone calls, or emails when trying to steal your goods or launder money.

There is also money laundering and terrorist financing. “Money laundering is the process by which funds derived from unlawful conduct are given apparent legitimacy - in essence cleaning the criminal proceeds. Terrorist financing is the process by which funds are gathered and used for terrorist activity”. International fraud is very common and happens all the time. We need to become more aware of fraud and how to recognize it, as well as take precautions to prevent it from happening. Fraud is more than just stealing money or products. Fraud can also be committed through international contracts. Some ways to prevent fraud in international business contracts include: getting expertise, employing letters of credit and securing payment methods, include requirement clauses in the contracts, becoming aware of current trends, and limiting the amount of security accesses within the business. If fraud is not your area of expertise, it may be beneficial to look for someone who is an expert in that field. A lawyer who has experience in the market you are investing in, and also have experience in international trade would be a good individual to seek advice from. It is also important to make sure that the terms in your contract are stated very clear and secure. Letters of credit are beneficial because the bank guarantees that the seller will get their money from the buyer. These letters of credit do not get rid of fraud completely, but it helps in preventing it from happening. Putting requirement clauses in contracts are helpful because you know you are doing business with parties that are legitimate. It is important to be sure you are aware of current trends.

There are a several organizations out there to help you keep up to date on trends. The National Anti-Fraud Network (NAFN) is one organization. The NAFN is in place to protect the public interest. This organization offers lots of information such as data from a wide range of providers, practice examples of process, forms, and procedures, etc. The U. S. Federal Bureau of Investigation (FBI) also posts the most up to date fraud schemes and suggestions to prevent them from happening. It is also important to limit access to security, both physical and technical. It is important to remember to follow all of these steps when writing contracts for international trade and business. This is one of the easiest ways to prevent fraud from even happening. Other countries also have organizations in place to help prevent fraud. There are several organizations that have been established to help fight these crimes in the United Kingdom. The

National Crime Agency (NCA) and HM Revenue & Customs (HMRC) are two of these organizations that have been formed in order to help reduce the amount of fraud happening. The NCA's role is to protect the public from serious threats and bringing in the people who pose those big threats.

HM Revenue & Customs is an organization that is responsible for several different taxes including: environmental taxes, income tax, insurance tax, corporation tax, etc. These organizations have legal obligations that derive from the Money Laundering regulations 2007 and the Proceeds of Crime Act 2002 (POCA). For terrorist financing there is the Terrorism Act 2000, which is an act put in place to prevent terrorism (nibusinessinfo. co. uk). If you hear about fraud, or know of fraud happening in your workplace, there is a number you can call and anonymously report it. You can also report fraud online. The United States has several different organizations in place to help reduce international fraud. The most well known organization is the United States Federal Trade Commission (FTC). The FTC is an organization put in place to "protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity. " They provide information to consumers to help them notice, put a stop to, and avoid fraudulent activity. Their main objectives are to protect their consumers, maintain competition, and advance organizational performance.

The Artists Against 419 organization is a group of international individuals that are determined in fighting advance fee fraud, also known as "419" fraud and several other different online scams. Advance fee fraud, or 419 fraud, is where a scammer attempts to convince a victim that they will receive a large sum of money, or other reward for a small payment. The most important part of this scam is that they lure the victim into agreeing to an illegal transaction, so when they get scammed they will be hesitant about going to the law enforcement about the deal. They try to get the victim to meet them in a foreign country. By doing this, the victim feels vulnerable and hesitant to contact authorities. The Artists Against 419 organization helps the public become more aware and educated in online scams and how to notice, avoid, and report them. Artists Against 419 has a database that is used for automated retrieval of bank fraud.

The Anti-Phishing Working Group (APWG) is an association that focuses on extinguishing identity theft and fraud caused by email spoofing and phishing. Email spoofing is "the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. " This is an easy way to scam people because people are likely to open emails and links when they think it's coming from someone legitimate (search. security. techtarget. com). This group allows the public to discuss phishing and spoofing issues in a public forum. It also allows them to report any spoofing or phishing scams they may come across (apwg. com). There is also an organization located in Japan called the Japan Company

Trust Organization (JCTO). It is an anti-fraud organization that is designed to protect buyer and sellers from internet fraud. All buyers should check to make sure that the Japanese company has passed JTCO's inspections to avoid fraud. To get a company registered with the JTCO, the company must send in an application, and the JTCO will decide if it's legitimate before accepting. Businesses with criminal records will not be approved by the JTCO.

SCAMwatch is another organization used to educate consumers and small businesses on recognizing, avoiding, and reporting scams. This website gives you resources such as the latest news and alerts on different scams going on around the world. SCAMwatch has a form where you can report scams that you have come across. It also gives information on the different types of scams that are out there and what you need to look out for (scamwatch. gov. au). International Fraud Awareness Week is an organization that travels around the world hosting events such as conferences and seminars on different fraud topics. They have several organizations, businesses, and government agencies that support them including General Mills and Microsoft. It also gives you resources to start getting involved in fraud week (fraudweek. com). This is a great organization to be involved in.

In the United States of America, any company that is Publicly Traded, i. e. , has issued stock on the New York Stock Exchange (NYSE) or National Association of Securities Dealers Automated Quotations (NASDAQ), is required by the Securities and Exchange Commission (SEC) to have an Independent CPA firm audit their books at least annually, and write a letter attesting to the books are in order and financial statements are accurate. This is done to somewhat guarantee that the books are accurate and that no fraud is being committed and to make sure the company is adhering to generally accepted accounting principles (GAAP). GAAP is a group of accounting standards that are used for organizing financial information into accounting records in an appropriate way, summarizing accounting records into financial statements, and disclosing any supporting information.

The Foreign Corrupt Practices Act of 1977 (FCPA) "was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. " The anti-bribery provisions of the FCPA is in effect and applies to every United States citizen and specific foreign issuers of securities. When the enactment in 1998 happened, the FCPA anti-bribery provisions affected foreign firms, and also anyone who was involved in corrupt payments in the United States. There are accounting provisions that companies must meet in order to be in accordance with the FCPA. The provisions are to "(a) make and keep books and records that accurately and fairly reflect the transactions of the corporation and (b) devise and maintain an adequate system of internal accounting controls" (justice. gov). Another threat that contributes to the fraud problems are cyber security threats. Businesses must have systems in place to prohibit scammers from stealing data. Cyber security is important because it prevents important data from being stolen,

identity theft, extortion attempts, etc. There are several different types of cybersecurity threats. These include: ransomware, malware, social engineering, and phishing. Ransomware is a software that was made with intentions to extort money. This is done by blocking access to the computer system until it's paid. However, there is no guarantee that access will be gained by paying the ransom. Malware is another type of software that was made to get access into a computer without authorization. It can also cause a lot of damage to a computer. Social engineering is another scheme designed to trick an individual into giving out confidential information. Social engineering is often used with ransomware and malware. When social engineering and malware or ransomware work together, it makes an individual more likely to give in to the scam by clicking on links or downloading malicious programs or software.

In a case study done on Target's credit card breach, Teri Radichel gives us some information on what happened, and some critical controls that could have prevented this breach. In December 2013, Target had a cybersecurity breach. Over 40 million credit cards were stolen from Target stores across the nation. Target was attacked in several different ways. They had malware in their systems, had phishing attacks, and their network segregation was poor. Malware was installed on their vendor machine two months before the credit card breach even happened. When the scammers got access to their system, they installed malware on their point of sale systems as well. This software stored information from every credit card that was swiped. The credit card information was sold on the black market. Target's monitoring software notified Target of the attack, but there was no response. In result of this credit card breach, several Target employees lost their jobs, even high up employees such as the board of directors. Banks had to refund over $200 million. Target had passed their security audit, but these scammers were still able to get through their security to install the malicious software in their systems.

The federal government arranged for some public and private organizations to get together and form a list of critical controls that are used to prevent and detect attacks before they happen. There is a list of 20 critical controls, but a few of them include: Malware Defenses, Data Protection, Secure Network Engineering, Controlled Use of Administrative Privileges, Inventory of Authorized and Unauthorized Devices, Inventory of Authorized and Unauthorized Software, Wireless Access Control, and Data Recovery Capability. If Target had gone through this list of critical controls when designing their security software, it could have prevented the cybersecurity breach. International fraud should not be taken lightly. There are several resources out there to help fight fraud. It is important to be aware of the different types of fraud and to know how to spot, report, and avoid them. Every company should know what to do in case they come across fraud in their company. What would happen if a company got into fraud trouble and did not know how to deal with it? They could suffer a lot financially and even go out if business if the damage was bad enough. Companies should not be scared of fraud, but they should always be prepared and have precautions and implementations in place if it were to

happen.