Spring 5-19-2017

Illegal Insider Trading

Christian Presto
La Salle University, prestoc1@student.lasalle.edu

Christian Presto

Executive Summary 1

Introductory 2

Is investing in the stock market like gambling? 2

When Investing becomes like gambling 3

What is fraud? 4

What is material non-public information? 7

What is insider trading? 9

How to detect and reduce the risk of illegal insider trading 14

Separation of duties 15

Access Controls 18

Audits 22

Trading restrictions and approval authority 23

Documentation and reconciliation 25

Surveillance 30

- Email surveillance 31
- Intrusion and detection prevention system 32
- Machine learning - Exabeam 34
- Data loss prevention 36

Policy 38

- Tone from the top 38
- Educating employees 39
- Creating policies and enforcement 39
- Tip line 40

Case studies 40

- Raj Rajaratnam 41

Hackers 42

Lessons learned 43

Bibliography 44

Appendix 48

Executive Summary

According to the U.S. Securities and Exchange Commission illegal insider trading is defined as "buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. Insider trading violations may also include "tipping" such information, securities trading by the person "tipped," and securities trading by those who misappropriate such information." (US Securities and Exchange Commission, 2013). As time progresses individuals and companies are in need of the most current information in order to execute trading strategies. Some individuals and organizations are willing to pay others for insider information or even steal material non-public information in order to gain an unfair advantage over others in the market.

According to Donald Creesey's fraud triangle it is believed that the likelihood that someone will commit fraud is increased when they are pressured to commit fraud, there is an opportunity to commit fraud, and they rationalize the need to commit fraud. If we understand what may lead to someone to commit illegal insider trading we will be able to understand how to reduce the risk of illegal insider trading.

Based on professional experience with the protection of material non-public information and the surveillance of employee brokerage accounts, along with my academic experience in the Economic Crime Forensics program at La Salle University I will discuss the problems and costs that illegal insider trading has on society.

Ultimately this capstone project will present a guide for companies to use to build a surveillance program that will protect their material non-public information from those who wish to use the information to gain an unfair advantage. I will also propose methods as to how to detect, investigate, and mitigate the risk of illegal insider trading.

Introductory

Benjamin Franklin once said "An investment in knowledge pays the best interest". In the right hands investment in knowledge brings about innovation and prosperity. But in the wrong hands knowledge can lead to greed and the destruction of integrity. Illegal insider trading should be considered a crime because it fails to add value to the economy, it causes economic losses to victims, and the activity degrades market confidence which negatively impacts the economy. The New York Stock Exchange is just one of several stock markets in the world, but it is the largest with over $20 trillion in market capitalization as of December 2016 and billions of dollars in trading value averaging daily (NYSEdata, 2016, 2017).

Is investing in the stock market like gambling?

At face value a short answer to this is – no. Although both involve the commitment of money in order to seek a return and both involve a certain level of risk, gambling and investing in the stock market are not the same because the stock market involves investors purchasing a part of a company so that the company can use that investment to purchase capital to be used to create new products or to offer services. Gambling on the other hand does not involve investors purchasing part of a company that will need to purchase of capital to offer new products or services to the economy as a whole. Another difference between the stock market and a casino is the playing field. At a successful casino the odds are always stacked in favor of the house – this is how casinos are able to continue to operate; if the casino did not have favorable odds they would surely go bankrupt. In the stock market the regulators aim to make the playing field more level and require that certain information be disclosed to investors in a timely manner.

When investing becomes like gambling

Many would agree that in order to be a successful investor the investor must have done some amount of research which makes them more knowledge about the companies they wish to invest in. The success of the Stock Market depends on the integrity of financial statements made by the companies and also the integrity of those who are trading on the market. Unfortunately it should come to no surprise that where there is an opportunity to make a lot of money quickly there will always be people willing to take advantage of others.

According to U.S. Attorney Preet Bharara the focus of their investigations into securities fraud is due to "…a commitment to longstanding principles and goals: that our markets should be fair; that our playing fields should be level; and that our citizens' accounts should be secure". (Bharara, 2009). The success of the Stock Market depends on the integrity of others; if people are not confident in the integrity of the companies or the traders in the market they may be more averse to investing in the stock market. Companies would lose investment opportunities because of the lack of funding and the economy in turn would be negatively affected. Products and services that could change society may never reach the public because investors are averse to investing in a risky market.

Let's use the example of the gambling game poker. In this game cards are dealt and players must make a wager based on what information they have and what they think they know about the other players' hand. Whoever does not fold and has the highest hand will win the round. Let's imagine at this same game prior to any hand being dealt one of the players knows exactly which cards are going to be dealt and to who they are going to be dealt to. Would you still want to play against that player? Most likely not since that player has an unfair advantage –

they have access to information about how the game will play out before anything even happens; this is somewhat like illegal insider trading.

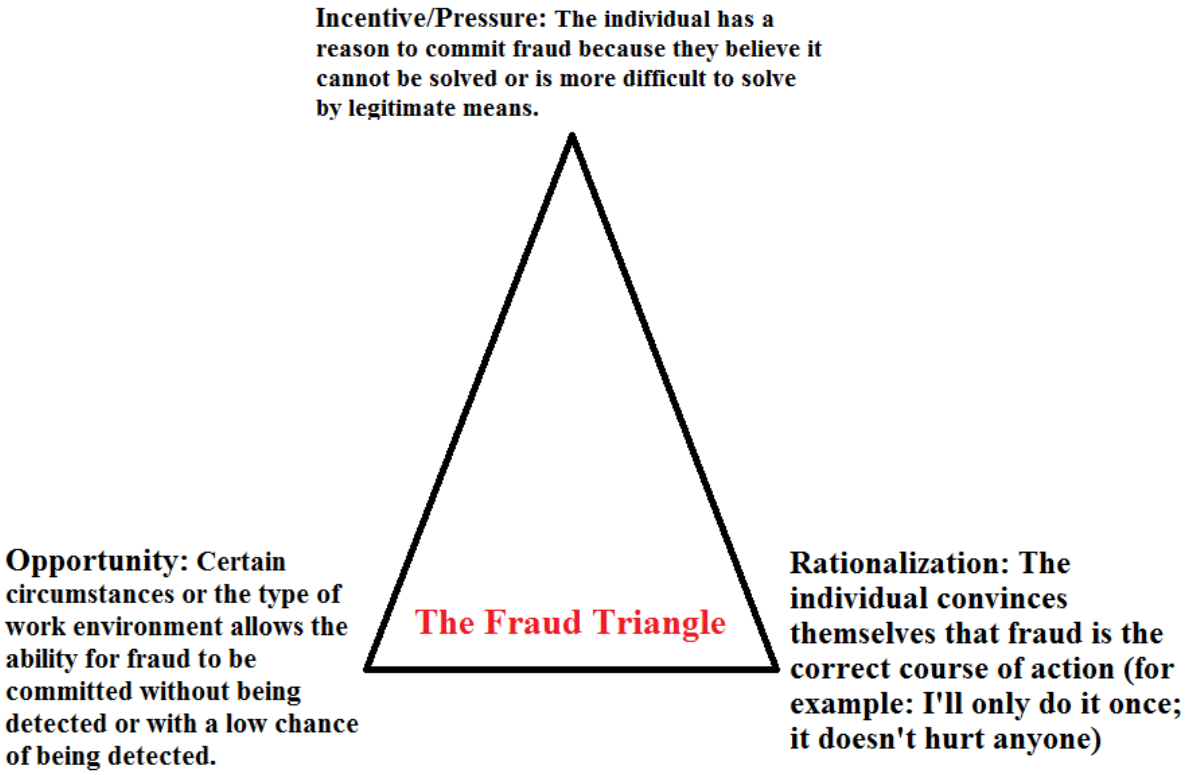
It is for this reason the Government and companies have stepped up their role to combat illegal insider trading. In this capstone project we will be able to understand why illegal insider trading is a serious crime, the reason why someone would do it, how to detect it, and how to reduce the risk of illegal insider trading.

What is fraud?

According to Black's Law Dictionary fraud is defined as "A knowing misrepresentation of the trust or concealment of a material fact to induce another to act to his or her detriment". We can go on to say that fraud is the intent to deceive another in order to reap an economic benefit or to avoid economic loss at the expense of a victim. Dr. Donald Cressey was a criminologist who focused on embezzlers and he developed what is known as the fraud triangle. The fraud triangle is broken down into three sections: pressure, opportunity, and rationalization. The fraud triangle was meant to help explain why someone would want to commit fraud. Pressure is the motivation that is behind committing the fraud, it is the reason why an otherwise law abiding citizen would go over the edge to commit a crime. An example of pressure could be if the individual was facing financial difficulties unsolvable through legitimate means. They may turn to alternatives such as stealing money, falsifying financial statements, or even obtaining insider information illegally. Financial problems such as too much debt or pressure to perform well in order to keep their job may be reasons why someone would be driven to commit fraud.

The second section in the fraud triangle is the opportunity. Opportunity is the ability for a person to commit a crime without being caught. The lower the risk of being caught then the greater the opportunity it is for someone to commit the crime.

The third section of the fraud triangle is known as rationalization. Most white collar criminals are first time offenders that often times view themselves as a victim or someone in a bad circumstance. The fraudster wishes to rationalize their behavior so that their crime seems justifiable. It is for this reason an otherwise law abiding citizen would be driven to commit a crime at the expense of others. For example a trader may trick themselves into believing because they are not causing harm to people and because they are not lying to someone illegal insider trading is a victimless crime.



But is insider trading really a fraud that should be considered illegal? Are there really victims of illegal insider trading? An article written by Melissa Robertson of the Securities and Exchange Commission mentions a few arguments that people have that oppose prohibiting insider trading; she mentions that most of these arguments fall on their own weight.

The first argument is that "insider trading is a legitimate form of compensation for corporate employees, permitting lower salaries that, in turn, benefits shareholders…This argument, however, fails to address the real and significant hazard of creating an incentive for corporate insiders to enter into risky or ill-advised ventures for short term personal gain, as well as to put off the public release of important corporate information so that they can capture the economic fruits at the expense of shareholders". In other words it is no excuse to engage in illegal insider trading because an insider feels entitled to reap the benefits from information they have a fiduciary trust in. The information which is material should be disseminated to the public before they themselves can trade in their company's securities.

The second argument is that "American reliance on several antifraud provisions, and the absence of a statutory definition of insider trading, may lead to unfairly penalizing traders whose conduct comes close to the line…This seems an illusionary concern. First, scienter, a fraudulent intent is an element that must be proven. Second given the inherent difficulties in investigating and proving insider trading cases, the reality is that there is a significant amount of clearly illegal activity that goes undetected or unpunished". In other words in order to charge someone with fraud it must be proven that there was intention to deceive others. The case studies referenced in this capstone project will allow us to see that the insider traders knew that the information was material nonpublic information and decided to act on that material nonpublic information in order to reap a benefit at the expense of others.

The third argument is that "…insider trading is a victimless offense and that enforcing insider trading prohibitions is simply not cost effective; the amount of money recovered does not justify the money and human capital spent on investigating and prosecuting insider traders…This penny-wise, pound-foolish argument neglects the external costs that result from a perception that insider trading is unchecked…governments cannot afford to turn a blind eye to insider trading if they hope to promote an active securities market and attract international investment…one of the main reasons that capital is available in such quantitates in the U.S. markets is basically that the investor trusts the U.S. markets to be fair. Fairness is a major issue. Even though it sounds simplistic, it is a critical factor…" Again we see that the success of the U.S. markets depends on how the investors perceive the fairness of the playing field. If the market appears too risky because people are fraudulent then people are going to be less likely to invest in the market. This in turn affects legitimate companies that are trying to raise capital to build their company.

Referencing the definition of fraud we can see that the insider has a knowing misrepresentation of trust or a concealment of material fact. When we look at the fraud triangle the insider is acting only to benefit their own interest because their problem is non-shareable; they feel that they must commit fraud in order to solve some financial pressures that cannot be solved through legitimate means. The opportunity to commit illegal insider trading arises due to too few controls and the rationalization to commit illegal insider trading arises due to people viewing it as a victimless crime and the benefit outweighs the punishment.

What is material non-public information?

According to Black's Law Dictionary something is "material" when it is important, more or less necessary; having influence or effect; going to the merits". (Black's Law Dictionary,

1910). Other sources define "material fact" as "a fact that would be important to a reasonable person in deciding whether to engage or not to engage in a particular transaction; an important fact as distinguished from some unimportant or trivial detail". (Lectic-Law, 1995-2017). So is illegal insider trading a victimless crime? After all – no physical harm is done to anyone and it isn't like a Ponzi scheme where investors are lied to and cheated out of their investments.

Illegal insider trading should be considered a crime because the act does not add any value to the economy and more importantly the results are losses to victims and the degradation of market confidence. Illegal insider trading does not benefit the economy as a whole because the activity is not offering a product or service to benefit consumers – the activity does not add value to the economy. Secondly traders add value to the economy through the movement of securities from low demand to high demand. Essentially traders use the same amount of information that the general public has access to in order to move money through the economy as efficiently as possible by making investment decisions based on research. Those who engage in illegal insider trading on the other hand are in possession of material non-public information that gives them a significant advantage over the market; essentially in illegal insider trading only a few individuals are able to benefit while the market as a whole suffers because information is not equally shared. Instead of all the traders being able to access that information to efficiently move money through the market they will always be beat by someone who has access to that material non-public information before they do. If the market loses its confidence then that would certainly lead investors to exit the market since they would always be at a disadvantage to those trading on material non-public information. A domino effect would ensue as more investors leave the market leading to less capital being invested, which in turn would make it

more difficult for entrepreneurs to raise capital to introduce a good product or service to the market. The economy as a whole would certainly be affected.

The fact is that there are people with non-public information which if known to the public would certainly affect the trading. Those who possess material non-public information are in a position of trust (fiduciary duty); their duty is to the shareholders of their company. In cases of illegal insider trading those who possess non-public information may choose to exchange their information for compensation (such as money, cars, jewelry, other favors) without releasing the information to the public first. The person who is purchasing the "tip" is essentially bribing the insider to gain information ahead of the rest of the market; this is creating an uneven playing field in the market and it is a breach of fiduciary trust.

What is insider trading?

According to the Securities and Exchange Commission the legal version of insider trading is when "…corporate insiders-officers, directors, and employees-buy and sell stock in their own companies. When corporate insiders trade in their own securities, they must report their trades to the SEC…Illegal insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security". (SEC.Gov, 2013). Illegal insider trading is acting on information which is not widely known to the public. Illegal insider trading is achieved when sensitive material information is either shared with another or it is stolen before the information is disseminated to the public.

An example of illegal insider trading would be if a company insider, such a majority stock holder, management, company's lawyer, research developer, accountant, etc… decided to

meet an investor for dinner to share an insider secret. The company insider has knowledge about the specifications of a new product; for example the next IPhone. The insider knows that the new IPhone will have parts specifically designed by another company. The Apple insider may offer to sell their knowledge about the specific company that Apple is going to do business with. The investor decides to pay the Apple insider for the tip and the next day the investor decides to purchase an enormous amount of shares in the company that will be manufacturing parts for the IPhone. Months later Apple releases press releases about the new IPhone, the specifications, and the companies that are manufacturing the different parts. People learn through the media about the companies and materials that will be used to manufacture the newest IPhone and they decide to invest in those companies. The stock prices will begin to drive upwards because people believe that the newest IPhone will surely sell millions so they want to invest in companies that are directly involved in the manufacturing of the new phones. The investor who paid a bribe for the material non-public will make a huge profit after selling his shares because of the inside information that he had before it was released to the public. This trader did not add anything to the economy and he caused other investors to pay more for the stock even though if it was a leveling playing field they shouldn't have. The trader also bribed the tipster; the tipster accepted the bribe and he violated his fiduciary trust with the company. This is why this type of activity should be considered a crime.

In the same way an investor can also have inside information that would cause them to sell before the bad news reaches the public. For example let's say an investor approached a company executive looking for investment tips. The company executive says that for some money he can tell the investor how he should trade in the company. The investor agrees to pay for the material non-public information. The executive says that the clinical trials of their new

drug have been a failure, they are going to cancel the project, and the company is not going to meet annual earnings expectations. This type of news would mean the company is bound to take a loss in profit and share price. If any investor knew that information they would most certainly sell the stock in the company. The investor decides to sell his stock in the company to avoid significant losses before the news is released to the public. A few months later the company goes public with a press release stating how the company will no longer continue developing the drug and how they have missed their annual earnings expectations. This causes other investors to panic and begin to sell their shares in the company. The stock price plummets and those who acted too slowly lost a lot of money. The issue in these two cases is that someone had an unfair advantage over others in the market because they were bribing company executives to divulge information that was not yet released to the public.

An article in "Kiplinger" by Kathy Kristof provides examples of what illegal insider trading is, what isn't illegal insider trading, and what may be a grey area that is best to avoid. The first example:

> "You are standing in line at Starbucks, and a well-dressed couple in front of you is talking about retiring to Majorca after they sell their company. You recognize them as the founders of a publicly traded company and figure out that the deal hasn't yet been announced. You snap up as many shares as you can afford and make a killing when the takeover is announced. Is this insider trading?
>
> No. If this couple bought or sold shares -- or called you and tipped you off in private -- it would be a violation. But illegal insider trading requires that you not only trade on the basis of important nonpublic information but that you also have some sort of duty to keep the information confidential. Former football coach Barry Switzer was sued for insider trading following a similar scenario in 1981, but he won the case because he had no duty to ignore a conversation he overheard in a public place." (Kristof, 2011)

In this first example the couple would be engaging in illegal insider trading if they purchased or sold the shares on their own or tipped someone off in private. However if someone overhears a conversation in a public space there is no reasonable expectation of privacy and the individual overhearing the conversation was not in a fiduciary duty for that information.

In the second example we see that expectation of privacy plays a major factor in determining whether acting on a "tip" is illegal insider trading or not.

> "You're a janitor at a major company. You hear members of the company's board convening outside the room you're cleaning and decide to hide in the closet. The board okays a deal to sell the company for a fat premium to the current share price. You load up on the shares. Illegal insider trading?
>
> Definitely. This is not a public place, and "you'd be in a position to understand that confidential information was being disclosed, which changes the calculus," says Andrew Stoltmann, a Chicago-based securities lawyer". (Kristof, 2011)

This second example is different from the first because the janitor was in a place where there was a reasonable expectation of privacy. He is not on the board and he was not invited to that meeting; therefore he is not allowed to hear that non-public information until it is released to the public. Since the janitor acted on material non-public information he was not allowed to hear he engaged in illegal insider trading.

In the third example the sources that are used makes a difference as to whether someone is engaging in illegal insider trading or not.

> "You're a hedge fund manager, and you pay dozens of analysts and consultants to provide seasoned advice about stocks to buy and sell. Some of those consultants may have access to secret information, but you trade based on a wide array of factors, including examination of public documents and detailed analysis about industries and companies operating within them. Insider trading?

> This situation probably would not be considered insider trading. The key to the case against Galleon CEO Raj Rajaratnam, says Stoltmann, hinged on whether his lawyers were able to establish that his trading was based on assembling a "mosaic" of information or whether he paid "consultants" to feed him insider tips. The former, says Stoltmann, is perfectly legal. The latter is not." (Kristof, 2011)

If a trader is basing their trades on material non-public information then it certainly would be illegal insider trading. But if they base their trades on research performed and the references is public information then the action would be legal. Where an individual gets their information from can certainly mean the difference between legal and illegal.

The above examples aren't the only ways that material non-public information may be obtained. In this age of technology cyber criminals are doing more than just stealing personal information and accessing bank accounts; they are also breaking into companies' computers in order to steal material non-public information. That information may prove invaluable to a cybercriminal because they could know a company's business strategy, specifications for their products, and test data. A cybercriminal could either sell this information to investors or they themselves could use this information to gain an advantage in the stock market. This type of behavior is detrimental to the stock market because it undermines investor confidence in the market. In one article published by the Department of Justice nine people were charged in a scheme to steal material non-public information.

> "The indictments unsealed today charge the defendants with hacking into the newswires and stealing confidential information about companies traded on the NASDAQ and NYSE in what is the largest scheme of its kind ever prosecuted. The defendants allegedly stole approximately 150,000 confidential press releases from the servers of the newswire companies. They then traded ahead of more than 800 stolen press releases before their public release, generating millions of dollars in illegal profits.

> "The defendants were a well-organized group that allegedly robbed the newswire companies and their clients and cheated the securities markets and the investing public by engaging in an unprecedented hacking and trading scheme," U.S. Attorney Fishman said. "The defendants launched a series of sophisticated and relentless cyber attacks against three major newswire companies, stole highly confidential information and used to enrich themselves at the expense of public companies and their shareholders." (Department of Justice NJ, 2015)

This case example demonstrates the need to not only ensure that employees aren't leaking material non-public information but that databases which house material non-public information is also protected.

We can come to understand that illegal insider trading is a fraud because there is intent to deceive others (albeit not up front) with the goal of a monetary gain or to avoid monetary losses at the expense of victims (those who do not yet have access to the same information). For this reason it is in the best interest of companies and the Government to implement controls to detect and deter the illegal acquisition of material non-public information and illegal insider trading.

How to detect and reduce the risk of illegal insider trading

Material non-public information can be illegally obtained either by someone leaking it or by someone stealing it. In order to detect illegal insider trading we must understand what would motivate someone to commit this crime. Going back to Donald' Creesey's fraud triangle we come to understand that a white collar criminal may engage in fraud because they are under pressure, there is an opportunity to commit the crime, and they rationalize the commission of the crime. If we wish to be able to detect and reduce the risk of illegal insider trading we must be able to address each of these sections in the fraud triangle. We can do this by ensuring these internal controls are in place:

1. Separation of duties

2. Access controls
3. Audits
4. Trading restrictions and approval authority
5. Documentation and reconciliation
6. Surveillance
7. Policy

Separation of duties

According to the American Institute of CPAs separation of duties is defined as "a basic building block of sustainable risk management and internal controls for a business. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. Without this separation in key processes, fraud and error risks are far less manageable". (Ghosn, Segregation of Duties)

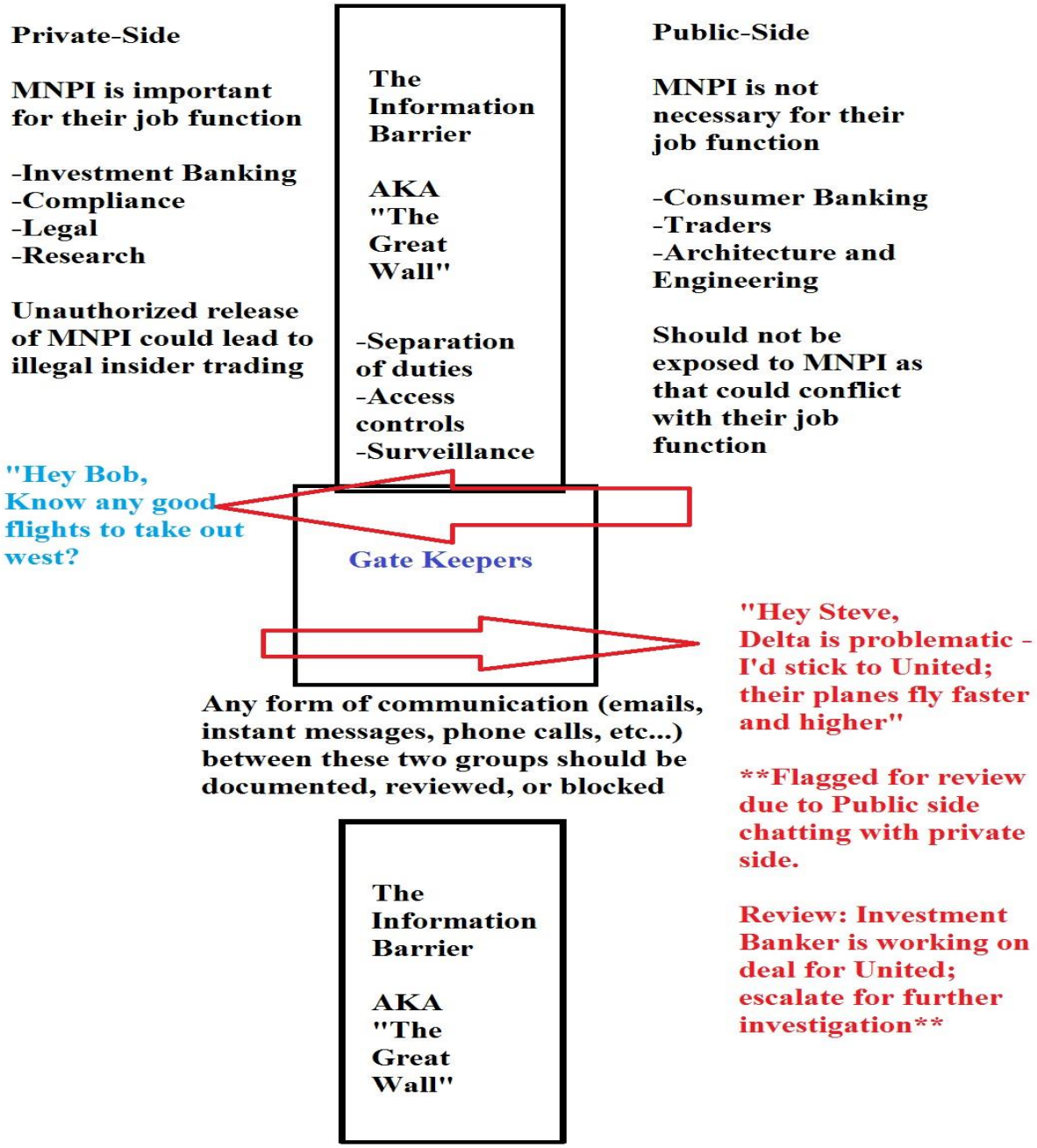
If one person had control over an entire system there is a significant risk that the individual could engage in fraud and conceal their fraud. The opportunity to commit fraud without being detected would be a motivating factor to cause someone to commit fraud. There are numerous examples of frauds going unnoticed for several years because an individual had complete control over an entire process without any oversight. The importance of separation of duties should also be extended to those who work with information. Giving someone unlimited access to a company's information could lead to disastrous results such theft or illegal insider trading. In the financial world some banks may divide their business into two categories: public side and private side.

In the public side, employees are not allowed to have access to material non-public information. Due to the nature of their jobs having material non-public information could

influence their decisions or make the appearance that they are not acting in the best interest of their clients. Examples of employees working on the public side are people in consumer banking (employees who work with individual customers rather than corporations; they assist with customers to open up savings accounts, loans, mortgages, credit cards, investment accounts) or traders (people who take orders from clients and trade on behalf of their clients). If these employees had material non-public information in their possession they may be tainted to trade a certain way based on what they know about the company rather than what the customer wants. For example let's say these public employees did have material non-public information and they knew that their company was going to buy out another company; usually the acquiring company's stock will increase and the stock of the company being acquired will decrease. The customer wishes to sell stock in the acquiring company but purchase stock in the company being acquired (keep in mind the client does not know about the acquisition). In a fiduciary duty the employee should not share information about the acquisition; but they may be pressured to advise the client that it is a bad decision. The employee may feel the need that in order to make a better profit they should advise against the customer's decision. This conflict is a reason why public side employees should not be allowed access to material non-public information. The employee would be split between advising their client and also protecting the material non-public information; this is why public employees should not be exposed to material non-public information.

On the private side these employees are exposed to material non-public information; some groups on the private side would be investment bankers (people who work with mergers and acquisitions of other companies for example), legal (people who are exposed to company deals and litigation), or research (people who are researching products on behalf of the company

for business strategy) to name a few. In order for these individuals to successfully do their job they must be exposed to material non-public information. These individuals should certainly be scrutinized more with regards to what information they are exposed to, documentation of whom they meet, surveillance of communications, and surveillance of their trading accounts. Even within these groups the amount of information they have access too should be limited to the scope of their job. Someone in the investment banking side should not have communication with someone in the research business. For example let's say someone in the investment banking business didn't want bad press to be released about an acquisition (if it was released it would certainly hurt their business deal); the investment banker pressures the research business to publicize good press so that people do not sell out of the company being acquired but rather to continue to purchase to raise the value of the company being acquired. After the acquisition the investment banker is left with a more valuable acquisition than they would have had if the bad press was released. This is clearly an example of fraud because the investment banker is intentionally suppressing bad press (even though it is true) released to the public with the intent to deceive others, which causes other investors to act upon it, which resulted in a gain for the fraudster and a loss to the victims. The purpose of separation of duties is to ensure that employees are able to do their jobs effectively without exposing the company to the appearance of illegal insider trading.

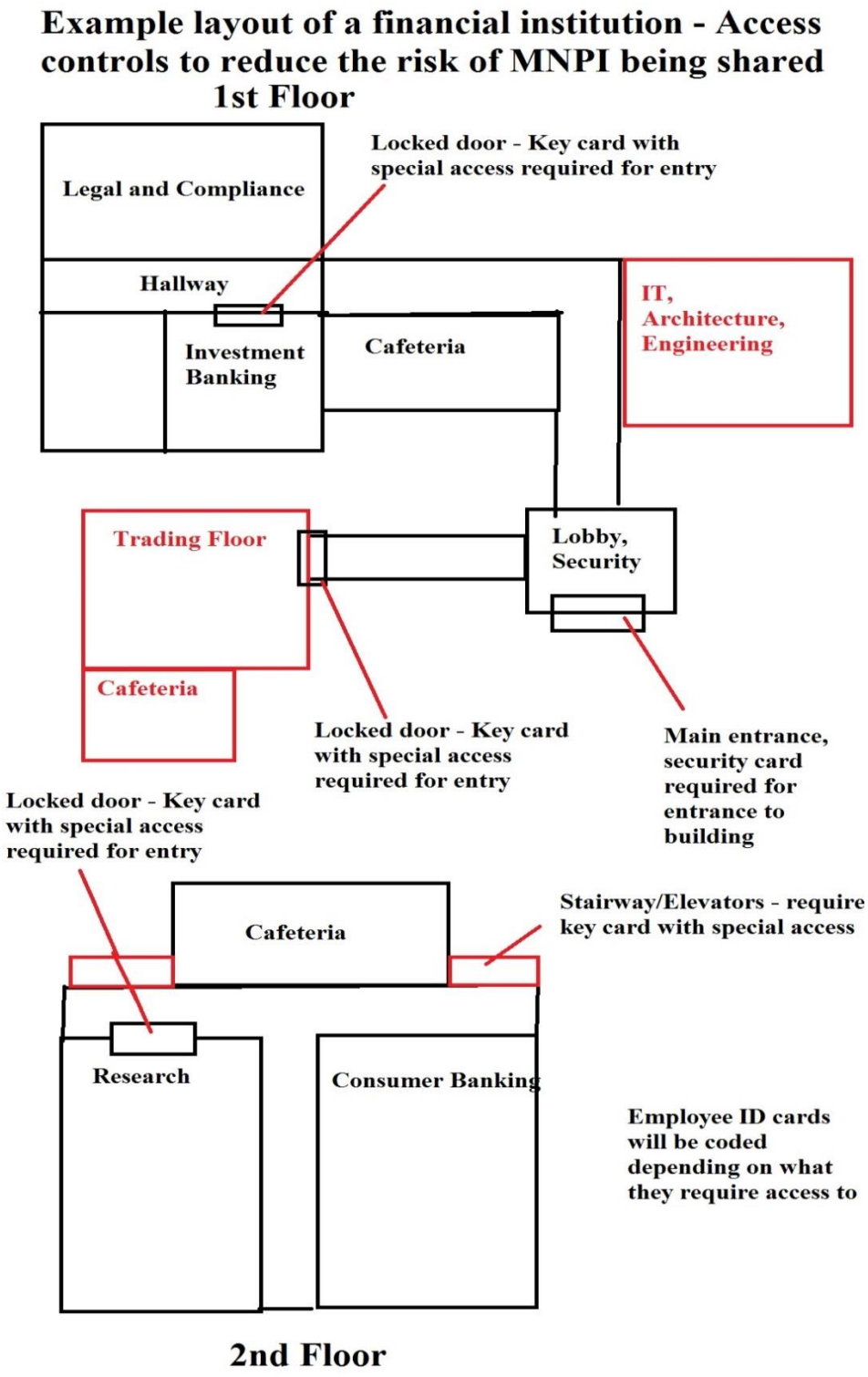


Access Controls

Access controls are like a gate in which only certain people that have permission are allowed to enter. Access controls can be both physical and also technological. As for physical access controls, in the financial industry for example, a company should have sensitive

information locked up, key card access to the building or rooms, the inability to download information from a computer to a USB drive or disk, and the presence of physical security guards. In certain companies physical access controls go even further by having certain areas of the company accessible only to certain employees. A company may have secured floors in a building accessible only by key card. In those areas only employees within that specific business are allowed to enter and sit next to each other. For example a company may not allow employees in the investment banking business to sit next to an employee in research by having the two different businesses physically separated. Employees may also be restricted to a certain dinning facility in the company – employees involved in research may only eat in one area of the company while employees in the investment banking are limited to another dinning facility in the company. If a company is much larger and has multiple locations it may even be more advantageous to have certain groups separated by physical distance. For example a company could have their investment banking department located in New York City, they could have their consumer bankers located across the country in branches only, and their compliance unit in Tampa Florida.

In a company the determination of how groups should be split up and who has access to certain floors should be determined and discussed by management. There should be a "Gatekeeper" that determines who has access to a specific area in the company and that access list should be reviewed by management and security at least annually to ensure that certain people have a specific reason to have access to that area.



Having a secured building is important in keeping unauthorized individuals out so that they cannot just walk into the building and steal what they want. But what if the individual can

get into the building legitimately? Remembering to physically lock up sensitive information in desk drawers or secured rooms is also equally important. Individuals that are not authorized to view sensitive information (such as a janitor or someone else) could steal that information and use it to their own advantage by either trading on it or by selling it.

It is also important that companies prevent employees from downloading information onto USB drives or onto disks. Inserting a device into a company computer poses a variety of risks; such as theft of information even to uploading a virus into the system. Physically preventing employees from doing this will reduce the risk that material non-public information can be stolen. In one case an advisor of Morgan Stanley Smith Barney conducted around 6,000 unauthorized searches on the bank's computer system and he stole client names, addresses, telephone numbers, account numbers, and other sensitive data. In response to Morgan Stanley's failure to protect customer data they were fined $1 million by the Securities and Exchange Commission. Not to mention the time and money spent to alert clients of the data breach, to change the account numbers, to patch the data breach, and also the reputational damage the company faced. (Robinson, 2016) The same could happen to a company if their material non-public information is stolen; they could be fined by the Government, lose prospective business deals, and suffer reputational loss.

Not only are physical access controls important but technological access controls are also important too. IT and management should work together to determine what information an employee can have access to on a computer or database. If information is relevant to perform a job then the employee should have access to it; but information which is not relevant to an employee's job then they should not have access to that information. IT and management should

have an access control list to regulate who has access to certain material and this list should be reviewed periodically to confirm if an individual still requires access to that information.

There may be a time when a private side employee may need to share MNPI with another employee in the public side. This would result in the public side employee crossing over "The Great Wall" (information barrier) in order to receive that MNPI. An example of this may be someone from the technology team being used to develop a new surveillance program to catch insider traders. During testing and development of the program the technology team may be exposed to certain information about employees, their trading habits, certain business deals. Due to this type of exposure the technology team would need to be brought over the wall in order to be able to do their job. A control group should review who is being brought over the wall, how long they will be able to stay in the private side, what types of activity they are restricted to, and what type of surveillance they are subject to. A cooling off period should also be instituted when someone is being removed from the private side to cross back over to the public side. This cooling off period will ensure that the information the employee has gained will not immediately be used when they are removed from the public side coverage (people usually do not forget easily, so a period of time should be allotted where they may be moved back over the public side but still restricted as if they were a private side employee).

Audits

According to the Institute of Internal Auditors internal auditing is defined as "…an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management,

control, and governance processes". (Institute of Internal Auditors) In other words audits assist a business to ensure that it is following their procedures. Audits are also able to provide feedback to improve processes if the company is not being compliant with regulations or if the company is inefficient. Audits are necessary to ensure that the access control list is up to date and that employees that no longer require access to material non-public information are removed from that access.

Not only should a company perform internal audits of their departments but they should also stress the need for managers of departments to do routine self-checks to evaluate whether their employees are following their written procedures and to make any updates as necessary. The managers should review processes with their employees and discuss with their teams if certain functions can be made more efficient. A manager should also set goals for their employees to cross train over other functions so that the team is better-rounded and fresher eyes are able to identify any issues which may have gone unnoticed. Having employees cross train and rotate job functions also makes it more difficult for an employee to have complete control over a process, that otherwise may have given the opportunity to commit fraud.

Trading restrictions and approval authority

In order to detect illegal insider trading and reduce the risk of insider trading companies should institute a compliance program that will set forth rules as to what employees can and cannot trade in and also which employees of the company must disclose their trading accounts. Going back to the difference between public side employees and private side employees a compliance program should define what employees should be covered under trading rules and how to regulate what they can trade in. Since public side employees should not have access to

material non-public information (since it would conflict with their job) they are at a lower risk of engaging in illegal insider trading; therefore it is more reasonable to not force public side employees to disclose their brokerage accounts for surveillance purposes. Private side employees who have access to material non-public information should disclose their brokerage accounts so that their accounts can be monitored for suspicious activity such as illegal insider trading.

Not only should certain employees disclose their accounts but their accounts must also be actively monitored and certain trades should be restricted. Let's say a company is engaged in a business deal with a technology firm. Employees that have a direct relationship in the technology field should not be allowed to buy or sell stocks for that specific technology firm in order to reduce the risk or appearance of illegal insider trading. This list of restricted stocks should be closely guarded and people that have access to this list of restricted stocks should also be closely monitored and restricted from trading as they have more access to what companies certain employees cannot trade in; anyone could take an educated guess and say that these are companies that have active business dealings not yet made public which is why they are on the restricted list. We will discuss more in the surveillance section as to how we can protect this type of information from a technology perspective.

A compliance program is only effective if there is a process for escalation and a way for the company to deter employees from engaging in certain forbidden activities. Escalation processes might involve actions such as a first violation notification being sent to the employee and to their manager detailing what company policy was violated, and how to avoid violating company policy in the future because further violations will be reported to HR. A second violation notification should involve the employee, their manager, and the compliance officer for

that department stating a second violation was issued, what policy was breached, how to avoid breaching policy again. The company should consider documenting the second violation in the employee's HR record so as to deter the employee from breaching company policies in the future. A violation recorded in an employee's HR record could affect being promoted within the company, bonuses, being able to transfer to another department, etc…This type of punishment should act as a deterrent for committing future violations.. A third violation may consist of the employee meeting with his manager, the compliance officer for the department, legal, and human resources. The employee may be notified with one final warning that further breaches of company policy may result in termination from the company. A third warning should be recorded in the employee's HR record in case legal action is brought against the employee or the company. It is critical that proper documentation of violations is maintained in case an employee is ever investigated by Government authorities. The Government may ask what steps the company did to detect, investigate, and reprimand the employee for their activities. If documentation is not properly maintained the Government may decide to fine the company for not maintaining an adequate compliance program that did not take industry violations seriously.

Documentation and reconciliation

Documentation is the process of recording important information so that it can be used for reference at a later time. Reconciliation is the process of making information consistent so as to ensure proper documentation of information. In order to detect and reduce the risk of illegal insider trading a company should properly document cases where material non-public information is being exchanged and also employees disclosing their trading accounts should also be documented. For example if two companies meet to discuss an acquisition the meeting minutes should be documented to include when the meeting took place, where it took place, who

was present, and what was discussed during the meeting. This is to ensure that material non-public information which is being discussed is properly documented. Documentation is crucial in order to protect a company from facing potential lawsuits and in the case of illegal insider trading proper documentation will shift the blame from the company to the individual that is engaged in illegal insider trading.

Documentation of outside brokerage accounts is also a requirement of FINRA. According to FINRA rule 3210:

"*(a) No person associated with a member ("employer member") shall, without the prior written consent of the member, open or otherwise establish at a member other than the employer member ("executing member"), or at any other financial institution, any account in which securities transactions can be effected and in which the associated person has a beneficial interest.*

(b) Any associated person, prior to opening or otherwise establishing an account subject to this Rule, shall notify in writing the executing member, or other financial institution, of his or her association with the employer member.

(c) An executing member shall, upon written request by an employer member, transmit duplicate copies of confirmations and statements, or the transactional data contained therein, with respect to an account subject to this Rule."

(FINRA Rule 3210, 2017)

In one example a company executive has concluded their meeting with another company; the stock is listed as a restricted stock that cannot be traded because the business deal has not yet been made public. If an employee wishes to trade in a certain stock is denied to do so because it is on the restricted stocks the compliance unit should look further to see if they had any communication with other insiders. If there is no evidence then there is less of a risk that they were trying to engage in illegal insider trading. The company properly documented the meeting and instituted a control to prevent illegal insider trading and the appearance of illegal insider trading.

In another example an employee from one company had a private meeting with an insider from another company which was not documented. The stock was listed on the restricted list to trade in so the compliance unit blocked the trade. This blocked trade escalated when it was determined that the individual had been communicating with an insider from another company. Upon further investigation it was determined that the two were meeting and the other company verified that sensitive information was being shared with the other individual. The due diligence of both compliance units will protect the companies from legal actions from regulators for not having sufficient controls to protect against illegal insider trading.

Reconciliation of employee's outside accounts is critical to the surveillance of employees' accounts. The reconciliation process will ensure that the compliance unit is accurately monitoring employee accounts. Reconciliation of accounts would include ensuring account numbers are accurate, employees are accurately associated to accounts, paper statements or electronic data is properly being documented and reviewed for suspicious activity. Going back to the different groups of employees, certain employees are restricted from purchasing certain stocks while others are not. It is important that the correct employee is associated to the account to ensure a proper review of the trading activity.

Since paper statements of brokerage accounts and/or electronic data would be reviewed it is important that the information is protected. Account numbers, account titles, trading habits, is all information that must be closely guarded. Paper statements should be locked away in desk drawers or secure rooms, and electronic data should be encrypted. Due to how quickly trades are being made and the need to catch suspicious activity much quicker the industry is moving away from the review of paper statements and are instead moving towards receiving the trading data electronically. For example let's say an employee engages in a trade they never pre-cleared and

it was a stock on the restricted watch list. The compliance unit would not be able to catch that trade until the monthly statement is produced, mailed to the compliance unit, and then finally reviewed. This could mean a violation is not detected until over a month after the fact. What if the employee engaged in other violations during that lag time? Would it be fair to dispense multiple violations of company policy over a month after the fact it happened? Shouldn't the employee have been at least notified of the first violation so they know not to commit another? What about the security of paper statements being mailed to the compliance unit? From the time the statement is printed and mailed, to when it reaches the post office, to when it reaches the company's mail room, to finally reaching the compliance unit that sensitive statement has been in contact with many people. Who's to say someone isn't going to steal that personal information? What about the cost of collecting and storing the paper statements? Imagine hundreds and thousands of paper statements are received a month; all of this takes up physical space! These questions are exactly the reason why compliance units and companies should move towards receiving electronic trading data rather than receiving duplicate paper statements in the mail. Certain companies such as "SS&C Evare" act as a third party between brokerage firms and compliance units. According to the company website "Evare is SS&C's financial service-based solution with a specialized focus in the data aggregation, normalization, transformation and delivery to and from financial entities…" (SS&C Technologies, Evare) Let's say an employee has a brokerage account at UBS Financial, they are a private side employee and they are required by the company to pre-clear their trade. The employee trades in a stock without pre-clearing, it is also a restricted stock they should not be trading in. That very night UBS Financial sends Evare an aggregate of data of accounts tagged as being associated to Company A. Evare sends that data to Company A to review the trading activity. The compliance analyst reviewing trading

activity for employees with UBS Financial accounts noticed that an employee did not pre-clear a trade. They also noticed that this specific stock they did not pre-clear was on a restricted list. On that same day the compliance analyst may issue a violation notification and they can also work with the broker to reverse the trade. The employee is now wiser about the company policy, Company A also protected itself by taking action against any appearance of illegal insider trading, and the employee also had their trade reversed quickly so they did not lose much money.

Company A could also take their compliance program farther by establishing a program where certain employees are auto-approved to maintain accounts at certain brokerage firms. These brokerage firms decided to cut out the middle man of Evare and send the electronic data directly to Company A in real time. The benefit to this is that the electronic data is real time – therefore if an employee executed a trade that was on the restricted list they would immediately be blocked from making that trade. No chance of the employee having to lose money on a trade that would have had to have been reversed. Another advantage to receiving electronic data is that the information can be manipulated more easily and trends can be identified. With paper statements it would be incredibly time consuming to try and input all of the data in a spreadsheet to determine if there are any unusual patterns of trading activity. With electronic data a compliance unit could monitor the trading habits of a business group over a span of a time to see if it is unusual.

Of course not every single brokerage firm is capable of sending their trading data electronically. It is up to the company's compliance program to determine how they want to move towards electronic only data. The company could put a ban on opening up new accounts at brokerage firms which do not send electronic data; this would eventually lead to the decline of paper statements being received as the company would try to push their employees to open up

brokerage accounts at firms which send electronic data only. Going back to firms which send data directly rather than through a third party; Company A could entice employees to switch brokerage firms by creating business deals with brokerage firms that would offer special benefits to Company A employees for opening up accounts at their brokerage firms. The push towards receiving electronic data rather than paper statements will certainly increase efficiency of reviewing trading activity and also decrease the opportunity for illegal insider trading as trends could be more easily detected.

Surveillance

In order to reduce the opportunity that someone has to engage in illegal insider trading a company must conduct surveillance and implement controls. Surveillance to detect and reduce the risk of illegal insider trading involves the review of employees' brokerage account trading activity, their communications, what information they are accessing, and how that information is protected. Let's first discuss how a company can monitor employee brokerage accounts so they can detect and reduce the risk of illegal insider trading.

Previously it was discussed in the documentation and reconciliation section that employees that are exposed to material non-public information must document their meetings and also disclose their outside brokerage accounts. A compliance program should establish a system where they receive trading activity in the form of duplicate paper statements and/or electronic trading data from brokerage firms. This is evidenced in FINRA rule 3210: "(a) No person associated with a member ("employer member") shall, without the prior written consent of the member, open or otherwise establish at a member other than the employer member ("executing member"), or at any other financial institution, any account in which securities transactions can be effected and in which the associated person has a beneficial interest."

In order to conduct adequate surveillance of an employee's brokerage account the compliance unit must receive duplicate copies of their brokerage account statements either in paper form or in the form of electronic trading data. The compliance unit should review the trading activity to see if the employee pre-cleared their trades to see if it was on the restricted list, and also to determine if their trading activity violated any company policies; for example not holding their company stock for a specified time before information such as quarterly earnings are released.

Surveillance can also come in the form of reading emails that are sent from company computers, reading chat logs, and listening into phone calls made on company devices. In one example an investment banker was using code words in email exchanges to a friend who engaged in trading in companies that were about to be acquired. (SEC, 2010)

In the email communication:

Poteroba: Keep me posted as to how * * * [m]any frequent flier miles you've got this far and how many you plan to get by Friday[.] Will be in Boston tomorrow[.] Plans for a trip look fine so far[.] Worst case we can get a refund by Monday, hopefully we do not[.]

Koval: As I mentioned, I just got into this frequent flyer program. I got five thousand of sign-in bonus miles but thinking maybe if I fly often, I will get additional three to five K miles.

Poteroba: On the frequent flyer program topic you mentioned, I think you should sign up for another flight, if you can, since they are providing bonus mileage soon[.]

In the SEC complaint Koval then wired $5000 into an inactive brokerage account and Koval purchased $2,100 shares of Guilford stock. Later on in the same month Guilford announced that it would be acquired by another company; this resulted in the stock price of Guilford to soar.

The suspicious email exchanges between the two and the suspicious activity of suddenly funding the account and purchasing a large amount of shares in a company that very quickly increased in stock price raised red flag indicators of insider trading. Koval had faced a 26 month sentence and agreed to foregut $1.4 million he made on his illegal insider trading activities. Poteroba agreed to forfeit more than $465,000 and was sentenced to 22 months in prison. (Russ, 2011)

This is an example of how an effective electronic communication surveillance program can detect and stop illegal insider trading.

It is important that a company protect its information from internal and also external threats. Previously we discussed how a company can conduct surveillance of employee's brokerage accounts and also electronic communications. It is also important that a company conduct surveillance and institute internal controls over the databases which house material non-public information. Since these systems store material non-public information they are targets of individuals who wish to engage in illegal insider trading. Protection from both types of threats include: Intrusion and detection prevention systems, user behavior analytics, and data loss prevention.

An intrusion and detection prevention system as defined by PaloAlto networks is "a system that is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network. Actions may include sending an alert to an administrator of the system, dropping malicious packets, blocking traffic from a source address, resetting connection." (Paloalto). There are two types of IDPS: Network-Based IDPS and Host-Based IDPS. A network based IDPS monitors traffic on the segment and it works to identify ongoing or successful attacks. A Host-Based

IDPS is placed on a specific computer or server and actively monitors activity on that specific system. When it comes to information security at a company it is best to have a layered approach rather than relying on a single tool to protect information. The network based IDPS is able to scan an entire network looking to detect external threats early on before they have a chance to access material non-public information. The Host-Based IDPS on the other hand is better suited to restrict and detect internal threats early on before someone has the chance to steal material non-public information. When it comes to protecting a database that houses material non-public information such as mergers and acquisitions, business strategies, and even the restricted stock list, a Host-Based IDPS should be utilized. The advantage to the Host-Based IDPS is that an administrator can establish specific rule sets for employees that have access to the system and they can monitor how much information they are accessing and at what times. This helps in the area of separation of duties; if a manager in the compliance unit wants a specific analyst to monitor one group of employees they can give them access to see what restricted stocks that specific group cannot trade in. While another analyst may be responsible for monitoring a different set of employees that have different trading restrictions.

The Host Based IDPS is also capable of documenting files which are accessed, altered, or downloaded and the time that these actions take place. This is helpful in identifying suspicious activity that is occurring on the host. For example if files are being accessed after normal business hours it should raise a red flag that someone may be accessing the information without authorization. Or if lists of restricted stocks are being downloaded it should also raise a red flag; the system should be set up to prevent files from being downloaded to avoid the loss of material non-public information.

Very recently there has been a great deal of interest in machine learning to help protect against information loss. According to the website SAS.com machine learning is "…a method of data analysis that automate analytical model building. Using algorithms that iteratively learn from data, machine learning allows computers to find hidden insights without being explicitly programmed where to look". (SAS, Machine Learning). Essentially this is a tool that can be used to detect abnormal activity on a network or on a host. The shortfall of Host Based IDPS is that an administrator must notice abnormal behavior and act upon alerts; but with machine learning the system can flag and also stop abnormal activity on a system itself. One such system is known as Exabeam; on the company's website it explains why the product is so useful "Cyber threats keep growing – they're more frequent and affect more people. Your security systems can't detect them, and your incident response teams are overloaded. .." (Exabeam). For around $25,000 the Exabeam system is able to perform an analysis as to what is normal activity and what is abnormal activity on a system. In performing it's analysis of user behavior it will create a scoring profile that asses the risk of the user's behavior. To better explain Exabeam will create a profile for a user based on what information they access, when they access it, from where, how often the access it. For example let's say a user only accesses their work from the company computer at the physical location sometime between 8:00AM to 5:30pm EST; if the same database is accessed from a high threat location of hackers, from the Ukraine for example, at a time not between 8AM and 5PM from a computer and internet service provider not recognized this would immediately raise a red flag and block the activity. Other uses of Exabeam could be combined with what type of information was accessed, what communications were sent, and the trading activity of the individual being monitored or the trading activity of individuals associated with the one who is being monitored.

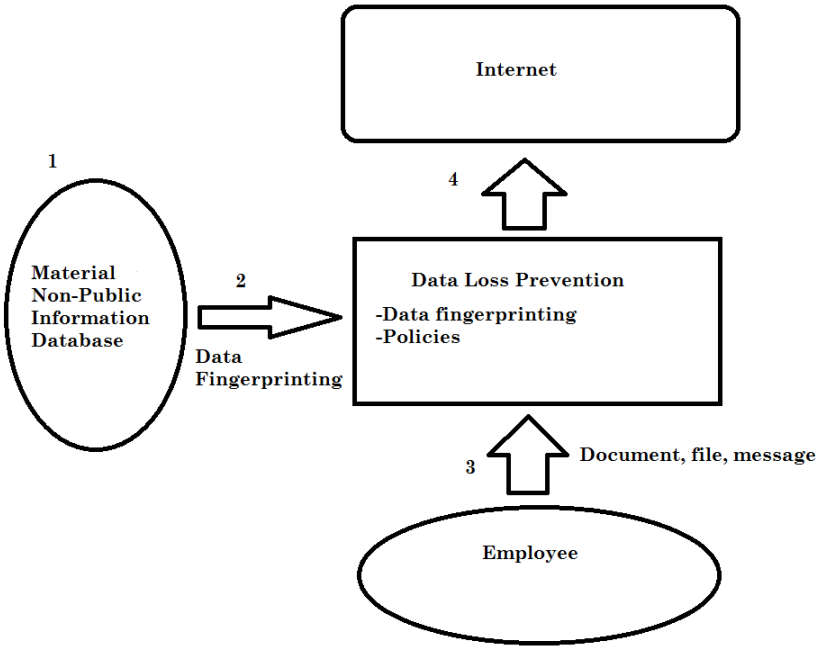
For example let's say a manager is performing an audit of users that have accesses to the restricted stock list. Using Exabeam they are able to look at the profile of the users and see who they communicate with and when they communicate with them. The manager can also review trading activity of those exposed to the restricted stock list and also review the trading activity of individuals that have been in communication with individuals with access to the restricted stock list. Let's look at the below sequence of events and see how Exabeam could be helpful in identifying and stopping illegal insider trading:

1. Employee from investment banking concludes a meeting with potential investors.
2. The company that he meets with is placed on the restricted stock list for certain employees because they are either directly or indirectly involved in the business deal.
3. The investment banker emails a friend in the research department and asks if he'd like to go fishing over the weekend. The friend agrees and so the two meet up over the weekend to go fishing.
4. While fishing the investment banker gives the fellow employee a tip that the company is about to score a major deal by acquiring another company. The employee decides it's a good bet to buy a lot of stock in the company that is being acquired because the share price will certainly rise once the news is released to the public.
5. On the following Monday the employee places a trade to purchase shares in the company that is being acquired. The employee contacted his compliance team to clear his trade. He is not blocked from trading in this security since technically he should not have been exposed to material non-public information about the company.
6. After the trade settles another compliance analyst is reviewing trading activity for the research employee and notices an unusual purchase of shares in a company that is

> restricted to trade in for employees in the investment banking business. The analyst decides to contact IT to pull up the Exabeam profile of the investment banker and they notice that in his history whenever he has a meeting with other company's he contacts his friend to arrange a meeting. The next market business day the friend makes a trade in a company that the investment banker has had a business meeting with. The company decides to investigate further and gather evidence of illegal insider trading.

This is just one of many examples of how a pattern of events could be recorded to identify unusual behavior; which would be: a meeting with investors, contacting a friend, friend places large trades in companies other friend is doing business with. A similar example could involve an employee always accessing certain data before it is released to the public, communicating a meeting with someone, and the employee's acquaintance trading large amounts just before the news is dispersed publically.

Another useful tool to aid in the protection of material non-public information is known as "Data Loss Prevention". According to Symantec data loss prevention is "…content-aware solution that discovers, monitors, and protects, confidential data wherever it is stores or used – across network, storage and endpoint systems". (Symantec SOS, Data Loss Prevention). Essentially this type of system that prevents sensitive information from being leaked out either intentionally or accidentally by users.



In the above example we can see how a simple data loss prevention program can prevent sensitive data from being leaked.

1. Sensitive information such as material non-public information will be stored on the company's database. Only certain employees are allowed to have access to this database and they are able to access information only relevant to their jobs.
2. The material non-public information is "hashed"; essentially a data fingerprint, which is a unique code, is created so that the information can be identified without actually making an exact copy of the data. The data fingerprint is then stored on the data loss prevention software.
3. The employee of the company decides to send out a message or file to the internet.
4. The Data Loss Prevention system stores the data fingerprints and also policies which determine what type of information may be released and what information must not be released. An example of a policy would be "Information regarding company X must not

be released between the dates of mm/dd/yyyy and mm/dd/yyyy". The system will scan documents being sent out by employees regarding a specific company for a specific time frame. Any documents that are being sent out will be scanned to see if it contains any information matching the data fingerprint. Information which matches the data fingerprint and policy may be blocked or come under review before being sent out over the internet.

Policy

In order to reduce the risk of insider trading a company must take a stance to remove the pressure that would cause someone to engage in illegal insider trading. They must also make illegal insider trading seem like a more irrational decision than not engaging in illegal insider trading. To do this a company should address these four points:

1. Tone from the top
2. Educating employees
3. Creating policies and enforcement
4. Tip line

Tone from the top according to Maureen Mohlenkamp and Nicole Sandford from Deloitte is "…an organizations guiding values and ethical climate. Properly fed and nurtured, it is the foundation upon which the culture of an enterprise is built. Ultimately, it is the glue that holds an organization together". (Mohlenkamp, Sandford). A company should establish policies which are in line with Government and industry regulations. Not only must they establish these policies but senior executives and other management should set a strong tone from the top. If a company has no policies then there is no way they can regulate what their employees are doing;

such as illegal insider trading. But even if a company has policies against illegal insider trading if the company executives are doing it then an employee could rationalize that it's okay to also engage in the illegal activity. Company executives must set forth an example for the rest of their company and they must also be held accountable for their actions. Therefore employees may be less likely to rationalize committing illegal insider trading.

Employees must also be educated on identifying what constitutes illegal insider trading and how to protect material non-public information. If employees are able understand why illegal insider trading is they should be less likely to commit the act (intentionally or unintentionally) and they should also be able to recognize red flag indicators of people engaging in the illegal activity. The more employees who are educated on identifying red flag indicators of insider trading the more difficult it will be for an employee to get away with illegal insider trading. Educating employees about illegal insider trading may involve a mandatory class when joining the company along with annual refresher courses. The company could also distribute memos and news articles about cases of illegal insider trading and the damage that illegal insider trading has on the economy and on companies.

The company must also create a balanced program that complies with regulations but is also a program that is workable for employees. For example if the company wanted to steer away from brokerage firms which do not send electronic trading data they could create a policy where accounts belonging to employees currently at these firms are grand-fathered in to be approved for them to be maintained. But employees are banned from opening up any new accounts at these specific brokerage firms. The logic behind this is that if all employees are forced to move their accounts (or accounts of those who are financially tied to the employee) from certain brokerage firms, employees may decide that the policy is too strict and that it is

more profitable for them to work at a different company with less strict policies. We could even go further to say that companies with policies which are too strict (such as banning employees entirely from opening or maintaining any brokerage accounts) may be a deciding factor for many prospective employees from accepting a job offer at the company.

The purpose of creating policy should be to develop an effective surveillance program that fulfills requirements of regulations but also appeals to the needs of employees. Policies must also be enforced by the company if they wish for their employees to take responsibilities for their actions. Violations of company policy and punishment must be tailored to the specifics of the case. If it is a first time offense and the offense was a low risk offense the punishment certainly should reflect that (perhaps a reminder of the policy and a discussion with their manager). But if an employee has violated the policy multiple times and the violation gave even the appearance of illegal insider then the punishment should be more severe (perhaps termination of the employee).

A company should also establish a reporting system where employees or people external to the company may be able to report suspicious activity of illegal insider trading without the fear of facing repercussion from individuals. The SEC also has a rewards program for people that report cases of financial crimes which lead to convictions. This is another way for companies to allow employees to be more open in reporting cases of illegal insider trading.

Case studies

Now let us look at two case studies one regarding a hedge fund manager that used contacts to get tips and another regarding a case of hackers stealing sensitive information. From

these case studies we will be able to understand why illegal insider trading occurred and how to prevent cases like these from occurring.

Raj Rajaratnam once a leading hedge fund manager of the Galleon group with a personal net worth of $1.3 billion was sentenced in May 2011 to eleven years in prison for illegal insider trading. Robert Khuzami, director of enforcement at the SEC described Raj Rajaratnam as "…not a master of the universe, but rather a master of the Rolodex". (The Economist, The Galleon Trial, 2011). The insider trading ring he was involved with included at least 20 people with around $72 million in gains and losses avoided. (The Economist, Schumpeter, 2011). Raj gained inside tips from people like Danielle Chiesi, who worked at a hudge fund group of Bear Stearns, Robert Moffat an IBM senior vice president, Rajiv Goel who worked for Intel Cpaital, and Anil Kumar who worked as a director of McKinsey and Company. (Dienst, McQuillan, 2009). The people that he used to gain material non-public information illegally were people that had a fiduciary trust to protect that information. Raj would pay for these tips using money and in exchange for material non-public information he was in possession of. Examples of stocks and profit's gained due to the scheme:

Stock	Profit
Google	$8 million
Akamai Technologies	$5.9 million
Hilton Hotels	$4 million
Sun Microsystems	$900,000
IBM	$500,000

It may be difficult to understand exactly what motivated Raj to engage in illegal insider trading but we could say that a lack of internal controls created the opportunity for Raj to engage in this activity. The reason why Raj was eventually caught was primarily due to a tipster reporting the activity to the authorities. From the tip received the FBI began to wiretap his conversations over a period of two years and they finally decided to make the arrest once they received a tip that Raj might being trying to flee the country.

This scheme may have been detected earlier on if the Galleon hedge fund had implemented the controls as listed above. Ensuring separation of duties and audits would ensure that Raj could not easily hide his illegal activities. Electronic communication surveillance may have been able to pick up suspicious communications with other corporate insiders outside of the company and those flagged communications could have been sent to a compliance unit that is reviewing the trading activity of Raj. The company could have also created an anonymous tip line and rewards system for employees or individuals that come forward about an illegal activity. By instituting better controls and policies the insider trading scheme could have been detected sooner and stopped long before investors were cheated out of millions of dollars.

In another case Chinese traders had hacked into U.S. computer systems of law firms that were responsible for handling mergers and acquisitions. The stolen information was then used by the traders to purchase stocks in the companies that were involved in the deals. Once the deal was made public the stock prices soared and then the traders sold the stocks which resulted in more than $4 million in profits from illegal insider trading. This case is interesting because cybercriminals are not only interested in stealing a person's identity, or stealing bank accounts, or other private information – hackers are also interested in stealing material non-public information to gain an advantage in the market. (McCoy, 2016)

It is crucial that companies invest in cyber protection to ensure that their systems are not brought down from a hacker but to ensure that their non-public information is not stolen. It is also important that these companies increase their cyber protection so as to protect themselves from facing lawsuits from clients and reputational damage. For example if company that was engaging in a merger had the deal leaked out because a law firm could not protect that sensitive information – then how likely would that business continue to use that law firm? Other businesses may also think twice about doing business with a firm that is unable to protect its sensitive information.

Some measures that a company should take would be installing a Host based IDPS to monitor and block suspicious activity. The company could also invest in a program such as Exabeam which would be able to identify normal activities and flag and stop suspicious activity. For example if Exabeam was used in this case the system may red flag a foreign IP address attempting to access the network. The system would log the activity but also ensure that the hacker does not gain access into the network. As a last line of defense the company should have also instituted a program such as "Data Loss Prevention" to ensure that a hacker could not click a few buttons to download volumes of material non-public information. The benefit in investing in these types of cybersecurity controls certainly outweighs the cost of being sued by clients and suffering reputational loss.

Lessons Learned

In conclusion illegal insider trading should certainly be considered a fraud because it is a violation of fiduciary trust which leads to some type of gain for the fraudster and a loss to the victims. Illegal insider trading degrades the integrity of our financial markets and will negatively

impact the economy. There are many ways that can lead to illegal insider trading, for example: employees sharing material non-public information to people that pay them for it, people stealing material non-public information that is not properly secured, hackers breaking into databases, employees purposely or accidentally releasing material non-public information onto the internet. Although there are many ways material non-public information can be released inappropriately a company can implement the following controls in order to detect illegal insider trading and also reduce the risk of illegal insider trading:

1. Separation of duties
2. Access controls
3. Audits
4. Trading restrictions and approval authority
5. Documentation and reconciliation
6. Surveillance
7. Policy

By implementing each of these controls a company can address each of the three sections of the fraud triangle (pressure, opportunity, rationalization) to make it less appealing and less likely for an individual to engage in illegal insider trading and to get away with it.

Bibliography

Bharara, P. (n.d.). Address on white collar crime. Retrieved February 06, 2017, from http://www.law.nyu.edu/sites/default/files/ECM_PRO_063924.pdf

Department of Justice. Nine People Charged In Largest Known Computer Hacking and Securities Fraud Scheme. Published August 11, 2015. Retrieved January 29, 2017. https://www.justice.gov/usao-nj/pr/nine-people-charged-largest-known-computer-hacking-and-securities-fraud-scheme.

Dienst, Jonathan. Alice McQuillan. Billionare Hedge Fund Founder Arrested for Insider Trading. Published October 16, 2009. Retrieved February 15, 2017, from http://www.nbcnewyork.com/news/local/Billionaire-Hedge-Fund-Founder-Arrested-for-Insider-Trading-64518027.html.

Economist, The. A massive insider-trading trial shakes Wall Street. Published March 10, 2011. Retrieved February 15, 2017, from http://www.economist.com/node/18334985.

Economist, The. Away with you. Published October 13, 2011. Retrieved February 15, 2017, from http://www.economist.com/blogs/schumpeter/2011/10/raj-rajaratnam%E2%80%99s-insider-trading.

Exabeam. Retrieved January 28, 2017, from https://www.exabeam.com/.

FINRA. 3210 Accounts at Other Broker-Dealers and Financial Institutions. Published April 3, 2017. Retrieved April 5, 2015. http://finra.complinet.com/en/display/display.html?rbid=2403&element_id=1228.

Ghosn, Anthony. Segregation of Duties. Retrieved January 29, 2017, from https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Auditing/InternalControl/Pages/value-strategy-through-segregation-of-duties.aspx.

Institute of Internal Auditors. Definition of Internal Auditing. Retrieved February 6, 2017, from http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-

auditing/?search%C2%BCdefinition.

Kristof, Kathy. Would You Be Guilty of Insider Trading?. Published May 2, 2011. Retrieved January 28, 2017, from http://www.kiplinger.com/article/investing/T052-C008-S001-would-you-be-guilty-of-insider-trading.html.

Lectic Law Library, The. Material Fact. Retrieved February 06, 2017, from http://www.lectlaw.com/def2/m021.htm.

McCoy, Kevin. Chinese traders charged with insider trading on hacked information. Published December 27, 2016. Retrieved February 15, 2017, from http://www.usatoday.com/story/money/2016/12/27/chinese-traders-charged-insider-trading-hacked-information/95874200/

Mohlenkamp, Maureen. Nicole Sandford. The First Ingredient in a World-Class ethics and Compliance Program. Retrieved January 16, 2017, from https://www2.deloitte.com/us/en/pages/risk/articles/tone-at-the-top-the-first-ingredient-in-a-world-class-ethics-and-compliance-program.html.

NYSE Group Shares Outstanding and Market Capitalization of Companies Listed. (n.d.). Retrieved February 6, 2017, from http://www.nyxdata.com/nysedata/asp/factbook/viewer_edition.asp?mode =tables&key=333&category=5.

Paloalto. What is an Intrusion Prevention System? Retrieved January 15, 2017, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Robinson, Matt. Morgan Stanley Fined Over Lapses Tied to Adviser's Data Breach. Published June 8, 2016. Retrieved January 8, 2016, from https://www.bloomberg.com/news/articles/2017-04-19/morgan-stanley-bond-traders-top-goldman-for-first-time-since-11

Russ, Hillary. Advisor Gets 2 Years For Trading On Ex-UBS Banker's Tips. Published May 24, 2011. Retrieved January 15, 2017 from https://www.law360.com/articles/246941/adviser-gets-2-years-for-trading-on-ex-ubs-banker-s-tips.

SAS. Machine Learning. Retrieved January 15, 2017, from ". http://www.sas.com/en_us

/insights/analytics/machine-learning.html

Securities and Exchange Commission. Published 28, 2003. Retrieved January 28, 2017, from https://www.sec.gov/litigation/complaints/comp18111.htm.

Securities and Exchange Commission. SEC Charges Securities Professionals in Insider Trading Scheme Using Coded E-Mail Messages. Published March 24, 2010. Retrieved January 15, 2017, from https://www.sec.gov/news/press/2010/2010-44.htm.

SS&C Technologies, Inc. Evare. Retrieved January 15, 2017. http://www.ssctech.com /Solutions/ProductsandServicesAZ/Evare.aspx

Symantec SOS. What is Symantec Data Loss Prevention?. Published on September 30, 2014. Retrieved January 28, 2017. https://www.youtube.com/watch?v=KIE1phfjiic

U.S. Securities and Exchange Commission. Insider Trading. Published January 15, 2013. Retrieved January 29, 2017, from https://www.sec.gov/answers/insider.htm.

What is material. (n.d.). Retrieved February 06, 2017, from http://thelawdictionary.org/material/

Appendix

Data Loss Prevention: A tool used to prevent the malicious removal or accidental removal of sensitive information from a computer or network. (Page 36, 37)

Donald Creesey: A criminologist who focused on embezzlers and developed what is known as the fraud triangle. (Pages 1, 4, 14)

FINRA (Financial Industry Regulatory Authority): A private corporation that acts like a self-regulatory organization that is meant to protect investors in the securities industry (See rule 3210). (Page 26)

Fraud Triangle: Created by Donald Creesey and used to explain why an individual would commit fraud. There are three parts to the fraud triangle; pressure, opportunity, rationalization. (Page 4)

IDPS (Intrusion Detection Prevention System): A system which is used on a computer or a network to identify unusual activity and to stop malicious attacks. (Page 32, 33)

Illegal Insider Trading: The act of trading on information which is not widely known to the public. (Page 9)

Insider Trading: When corporate insiders decide to buy or sell stock in their own companies. (Page 9)

Machine Learning: A tool which can learn the behavior of a user and make predictions as to what actions the user may take. (Page 34)

MNPI (Material non-public information): a fact that is important that if known to an individual would influence their decision making, but it is not widely known to the public. (Page 8)

Private-Side: Employees of a company that are exposed to MNPI in order perform their job function. (Page 16, Page 18)

Public-Side: Employees of a company that should not be exposed to MNPI because their job function does not require the use of it. Exposure to MNPI for public-side employees could create a conflict of interest. (Page 15, 18)

Rule 3210: A regulation set forth by FINRA which states that an employee of a member organization must seek approval from their employer prior to opening an account which transacts in securities. (Page 26)

SEC: Securities and Exchange Commission primarily responsible for enforcing the US federal securities laws.

SS&C: A third party company which specializes in data aggregation; one service the company provides is the secure transfer of trading activity in brokerage accounts to compliance teams for surveillance. (Page 28)