**Financial Fraud Risk Management**

**Description:**

The pillars of the American economy are organizations. One of the most urgent problems facing private enterprises is the lack of assets and the capacity to combat misrepresentation. Businesses that are more resistant to extortion could benefit both their owners and the overall economy. Regarding extortion, take a chance. As fraud experts, we have witnessed these confrontations firsthand and understand the suffering experienced by owners who unintentionally acquire a scammer's business.

The motivations behind extortion, however, can vary greatly across employees. While some may take from their bosses out of greed or necessity, others may defend their actions by claiming that they have earned the right to do so via their steadfast work and selflessness for the company. Private venture representatives who have played such a prominent role in creating the organization's resources may sense a tendency toward self-absorption. Additionally, representatives may defend accepting as a brief credit and justify their actions by stating that they have the best of intentions to pay back the entire amount before it is missed. Employee-related fraud can take many different forms, including the theft of company assets for the purpose of income skimming, the misuse of credit cards and other payment methods, time theft and other forms of financial extortion, and, surprisingly, intricate schemes to divert company funds through front companies or payoff deals with vendors.

As time goes on, criminals are increasingly using weak network security protocols at both large and small businesses to access vast amounts of sensitive customer data online. Information leaks may occur because of sophisticated programming flaws, but fraudsters can also use phishing to get employees of private companies to knowingly share this valuable information. Criminals have also been known to dig through trash or pose as a buyer, seller, or official to steal confidential information such as company account numbers (Hess,2016)

**Objective:**

* The main objective of this paper is to address the overview of risk management and focuses on the programs that are conducted by an organization that addresses fraud and misconduct.
* A fraud risk assessment is aimed at proactively addressing a business’s vulnerabilities to internal and external fraud.
* Though types of fraud vary by business line, internal frauds include embezzlement and misappropriation of assets, while external frauds include hacking and theft of proprietary information

**Fraud Prevention:**

* **Developing ethical culture:**

Most workers may not notice warnings or early warning signals since they have a very limited understanding of what extortion is. The effectiveness of your workers' moral motivation to raise concerns about any wrongs will determine how you respond to misrepresentation.

* focusing on certain topics, such as Clear Assumptions for What Is OK and Not OK
* Manifesting Desired Behavior
* Build the behavior you need, and don't encourage the behavior you don't
* **Internal control systems:**

A significant portion of cases of corporate extortion are discovered by workers. Representatives are given the tools to report thought-deceitful behaviors through a hidden hotline, an internal site or gateway, or another type of disclosing method. Various forms of internal control Controls that prevent fraud from happening; Controls that help identify and contain the harm caused by misrepresentation when it has already occurred; and Controls that address and correct problems that could lead to extortion, financial loss, or harm to the association's reputation.

**Fraud Detection:**

According to the ACFE, organizations should provide representatives and chiefs with training on misrepresentation awareness, according to the General Public for Human Asset, "These low rates show that numerous associations could not as yet comprehend the significance of proactive endeavors to help and urge tips to successfully recognize extortion." The board declared. At the absolute least, these programs should include instruction on what behaviors constitute misrepresentation, how extortion harms everyone in the organization, and how to report questionable activity. In addition to focusing on significant areas of strength for a counter plan, the board should not just invigorate detailing (Beaulieu-Volk, 2012).

**Responding to fraud:**

The Fraud Reaction Plan was created with the intention of directing representatives, directors, and the public in defining their roles in terms of activity and proclaiming lines in the event of thought extortion or degenerate action. Which includes the factors such as:

* Roles and Responsibilities
* Organizations dealing with fraud

**Cyber Risk Management:**

The board's regulations on network protection risk would oblige counsels and resources to adopt and put into practice plans and methods that are logically designed to counteract network protection risks. In order to assist in addressing operational and other risks that could harm warning clients and asset financial backers or result in the unauthorized access to or use of counselor or asset data, including the personal information of their clients or financial backers, the proposed rules list specific general components that counsels, and assets would be expected to address (sec.gov, ).

* Ongoing Process- Identify, analyze, evaluate, address threats
* Job od a security team
* Everyone plays equal roles
* Often business unit leaders view risk management from their business function
* The holistic perspective necessary to address risk in a comprehensive and consistent manner.



**Fig: Cybersecurity Framework**

**Risk Assessment:**

A risk assessment analysis has been conducted by taking the two financial sectors as examples and analyzing the potential hazards and impacts that could negatively affect the business's growth or success. Assessment is conducted by using any one of the risk assessment tools.

Two financial sectors chosen as examples

* analyzing the potential hazards
* impacts that could negatively affect

1. PayPal
2. Zelle

**Case-study: 1 PayPal**

The percentage of income that PayPal extorts is between 0.17 and 0.18 percent. While this percentage is significantly lower than the industry average of 1.86 percent, it really covers more than $1 billion in losses for the company each year. The platform combines massive amounts of data with ongoing processing, including customer signup, payment, invoicing preferences, and profile information. However, scaling the amount of information handled caused challenges due to a large important record, numerous petabytes of data, and a requirement to double the web-based exchange handling (OLTP) rate from 3.5 to 7 million exchanges per second (Pdf)

Approximately around 4.5 million fake PayPal accounts are being created so there are more chances for fraud.

some of the factors are:

* Advance Payment fraud
* PayPal account problems
* Overpayment refund scams
* Fraud involving delivery and payment cancellation
* Charitable-contribution and investment scams

**How can we avoid?**

* **Messages:** grammatical mistakes, attempts to incite a sense of urgency or danger
* Check any **potential issues** through your personal account on the website
* Not give out personal information to the other party

Graphical user interface, application

Description automatically generated

**Figure: 2 Risk Assessment for Scenario 1**

**Scenario- 1-2 ( How can we avoid risks)**

* **Even clients with legitimate credentials are capable of friendly fraud if they are impatient or ignorant. Insist on delivery signature confirmation when delivering expensive things.**
* **If you enroll in the Seller Protection Program offered by PayPal, some types of fraud will be paid for by PayPal.**
* **Customers who create fraud or dispute claims should be blocked. If no action is taken against a vendor, fraudsters frequently target them repeatedly.**
* **Check the actual email address rather than the sender’s name when you receive an in a new tab to double-check the details.**
* **Shipments must only be made to the address specified in the transaction details.**

**Graphical user interface, application

Description automatically generated**

**Figure: 3 Risk Assessment for Scenario 1-2**

**Scenario: 2 – Zelle**

* **Zelle, the popular payment app, is under fire for how it handles**
* **Zelle showed that fraud and theft are not only rampant but getting worse**
* **Banks are not repaying 90% of cases in which customers were tricked into making payments on Zelle.**
* **PNC Bank indicated that its customers reported 10,683 cases of unauthorized payments**

**Graphical user interface, text, application

Description automatically generated**

**Figure: 4 Risk Assessment for Scenario 2**

**Conclusion:**

* **Technologies for electronic payments present both potential and difficulties.**
* **The biggest obstacle to using online payments is fraud prevention and security.**
* **Two financial sectors are being analyzed for risk evaluation i.e., PayPal and Zelle**
* **PayPal prioritizes investing in the fight against fraud.**
* **With the safety measures, the primary losses and secondary losses are been decreased by approximately 20-30%**
* **For more than ten years, the business has used real-time decision-making in conjunction with effective fraud prevention methods.**
* **However, scammers are continually altering their strategies and finding new methods to abuse the system.**
* **Its always good to be aware of the risks by the frauds and take preventive measures.**

**References:**

Pdf (no date) PayPal solves fraud challenges, Intel. Available at: https://www.intel.com/content/www/us/en/customer-spotlight/stories/paypal-customer-story.html (Accessed: November 25, 2022).

Akhmedjanov, G. (2020). INFORMATION SYSTEMS SECURITY IN FINANCE USING MACHINE LEARNING.

*Fact sheet cybersecurity risk management - sec.gov* Available at: https://www.sec.gov/files/33-11028-fact-sheet.pdf (Accessed: December 1, 2022).

de Araújo Lima, P. F., Crema, M., & Verbano, C. (2020). Risk management in SMEs: A systematic literature review and future directions. *European Management Journal*, *38*(1), 78-94.

Sparks, E. (2018). Real-Time Banking: The Risk of Doing Nothing. *American Bankers Association. ABA Banking Journal*, *110*(5), 52.

Pdf (no date) *PayPal solves fraud challenges*, *Intel*. Available at: https://www.intel.com/content/www/us/en/customer-spotlight/stories/paypal-customer-story.html (Accessed: November 25, 2022).

Beaulieu-Volk, D. (2012) *Most common fraud detection method: Employee tips*, *Fierce Healthcare*. Available at: https://www.fiercehealthcare.com/practices/most-common-fraud-detection-method-employee-tips (Accessed: December 1, 2022).