FRAUD MANAGEMENT – A CASE STUDY

ABSTRACT

With the enhanced adoption of technology, The countries today are facing a significant problem with fraudulent activity, including financial fraud, identity fraud, and other types of financial activity with an intent to financially impact people. This case study provides an abstract to how technology can help overcome challenges faced by Organizations.

Vineet Bhargava

Founder, D2R Tech Private Limited

Introduction:

Technology today has brought the world closer. Specially post pandemic era, technology evolved and pushed people to adopt technology.

The Challenge:

With the enhanced adoption of technology, The countries today are facing a significant problem with fraudulent activity, including financial fraud, identity fraud, and other types of financial activity with an intent to financially impact people.

Fraudsters often use a variety of methods to commit technology fraud, including:

a) **Phishing:** This involves sending fake emails or messages that appear to be from legitimate companies or organizations, in an attempt to trick the recipient into revealing sensitive information such as passwords, credit card numbers, or bank account details.

b) **Malware**: This involves installing malicious software on a victim's computer or device, in order to gain access to sensitive information or to control the device remotely. Types of malware include viruses, worms, Trojan horses, and ransomware.

c) **Vishing**: This involves using the phone to make fraudulent calls, in which the caller pretends to be from a legitimate company or organization and tries to obtain sensitive information from the victim.

d) **Scams**: This involves tricking the victim into paying for fake goods or services, or into sending money to a fraudulent account. Common scams include fake job offers, lottery scams, and charity scams.

e) **Social engineering**: This involves manipulating people into divulging sensitive information or into performing actions that may not be in their best interests. It can involve tactics such as impersonation, pretexting, or influence.

The Solution:

While It is important to be aware of these methods and all countries are taking steps to protect their citizens and their information from such frauds. However, it is equally important for leaders of financial institutions governing the financial health of the countries to keep a continuous vigil and eye on patterns of such Frauds and enable an environment of prevention.

These malicious activities not only cause significant financial losses for the government and businesses in the country, but as well damages the country's reputation.

To address this issue, we partnered with an Indian company and implemented a comprehensive fraud prevention solution that included several key components:

a) **A centralized database of known fraudulent activity:** This database was used to track and monitor fraudulent activity across the country. It was populated with

information from various sources, including enforcement agencies and financial institutions.

b) **Engineering:** Engineering architecture was used to protect the sanctity of the information and allows access to only who are inside the organization whilst provision was to still communicate with outside world. A closed loop engineering architecture was used which allows Banks to send information to a central agency with real time jobs running to synch information as it was received so immediate actions can be taken. Tech stack used for building the solution is advanced and performs advanced engineering algorithm using *Angular JS*, *Node JS* as basic backbone of the tech solution.

c) **Advanced analytics tools:** These tools were used to analyse the data in the centralized database and identify patterns and trends in fraudulent activity. This helped to identify areas of high risk and target resources towards those areas.

This solution will not only keep a vigil on financial health of the country impacted by such frauds, but will also provide key insights like:

a) Victim demographics
b) Fraud Taxonomies
c) Fraud Channels
d) Mule Accounts and source of these Mule Accounts
e) How soon implemented solutions are able to detect such frauds
f) Preventive Guidelines implementations across financial Institutions

The Impact:

Question now comes is even if there are indicators and early signs made available, how would this information be used. At Policy level, These insights can help governments derive following actions:

a) **Collaboration with key stakeholders:** The governments can work closely with financial institutions, businesses, and law enforcement agencies to share information and coordinate efforts to prevent fraud.

b) **Public education and outreach:** The government can implement a public education campaign to inform citizens about the risks of fraud and how to protect themselves. This included information about how to recognize scams and how to report suspicious activity.

Finally, The Conclusion:

While it is imperative that at Policy level each financial institution governing countries finances are providing guidelines, putting frameworks, however it is equally important to keep a governance around those policies.
We can build solutions which can help Institutions implement IT enabled governance mechanism that can not only determine effectiveness of implemented Policies and frameworks, but also provide *Objective*, *Data Driven*, *Early Warning Signs* for preventing Financial Frauds.