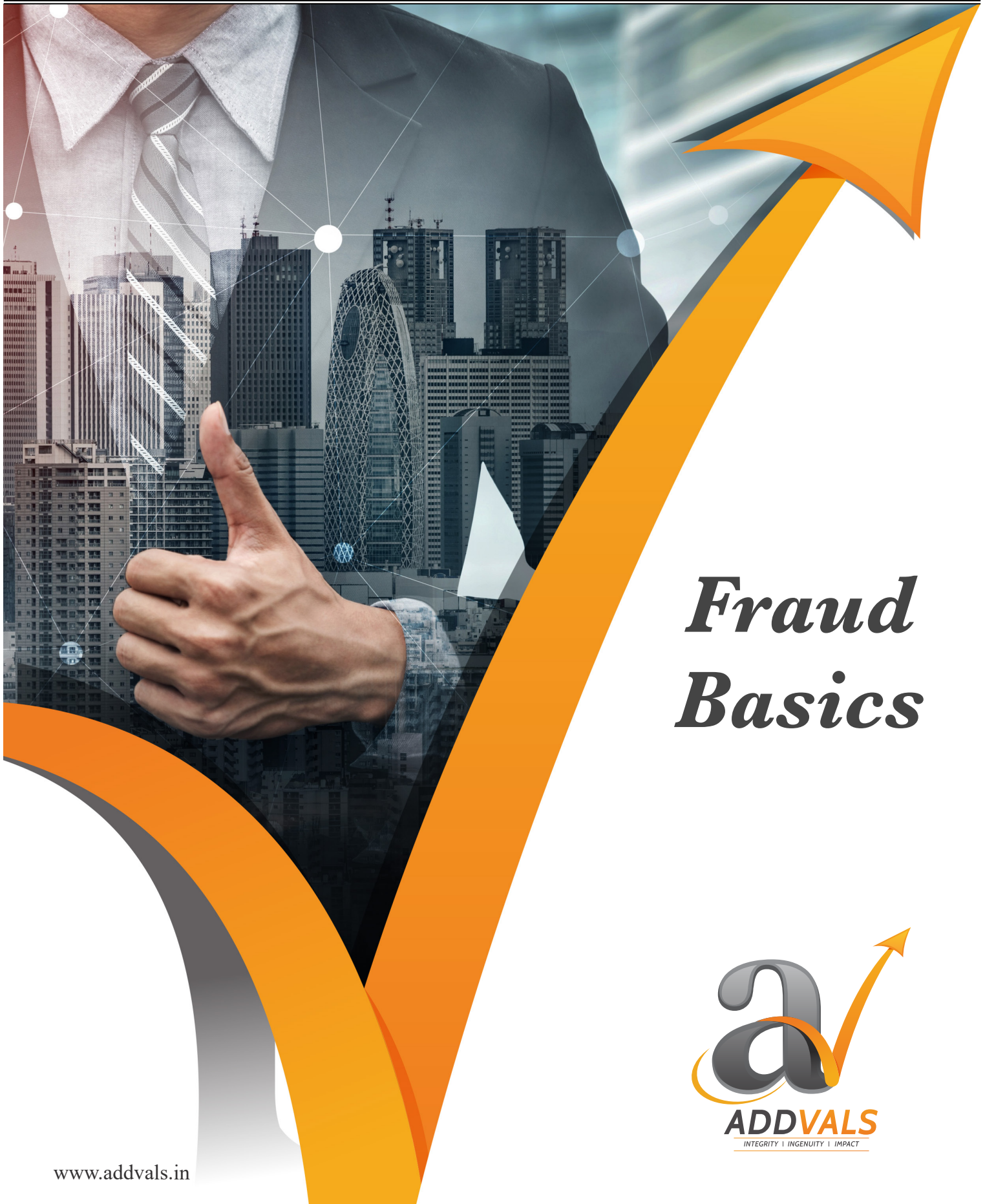


ADDVALS

Adding value by spreading knowledge

Volume 1, January 2023



Fraud Basics



INTEGRITY | INGENUITY | IMPACT

Insights in this Newsletter

01 What is fraud ?

02 Fraud Triangle

03 Fraud Tree

04 Fraud Scale defined by Steve Albrecht and his colleagues

05 Fraud-Vitta

Fraud Basics



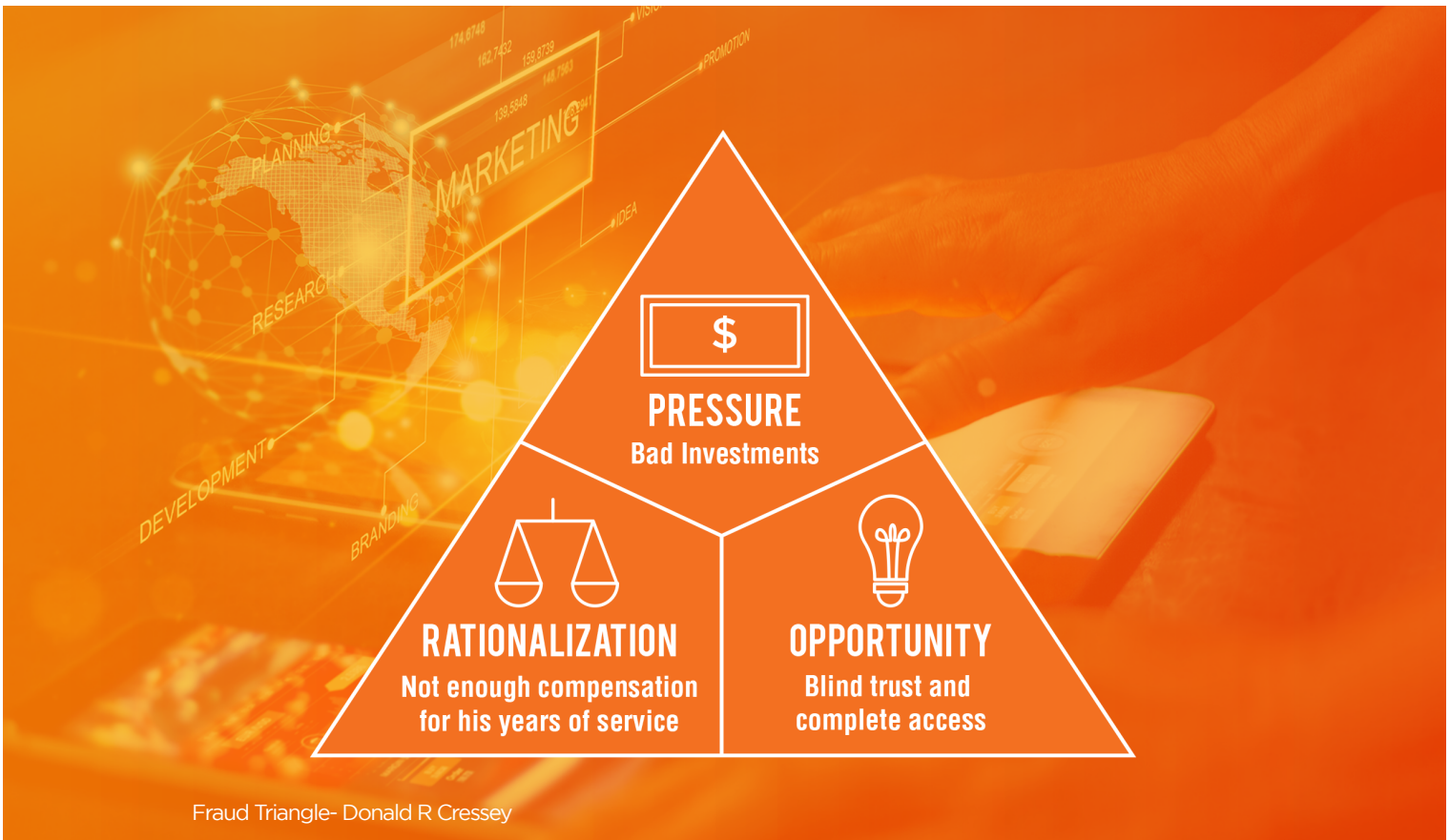


What is Fraud?

Fraud is any activity that relies on deception in order to achieve a gain. There is a very thin line of difference between fraud and error. Fraud includes the element of 'intent' while an error implies a mistake. Since, the person perpetrating a fraud conceals his trail, detection of fraud is difficult.

The explanation as per Companies Act, 2013, specifies "fraud" in relation to affairs of a company or any body corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss;

01



Fraud Triangle

is a framework used to explain the motivation behind an individual's decision to commit fraud defined by Donald R Cressey. It consists of three components:

- 1 Pressure:** Incentive, alternatively called pressure, refers to an employee's mindset towards committing fraud
- 2 Opportunity:** Opportunity refers to circumstances that allow fraud to occur. In the fraud triangle, it is the only component that a company exercises complete control over.
- 3 Rationalization:** Rationalization refers to an individual's justification for committing fraud.

Fraud Triangle is illustrated with an example

Mr. Shyam, an accountant, had complete access and authority over the company's credit cards and bank accounts. His long years of service to the organization made him a trusted employee.

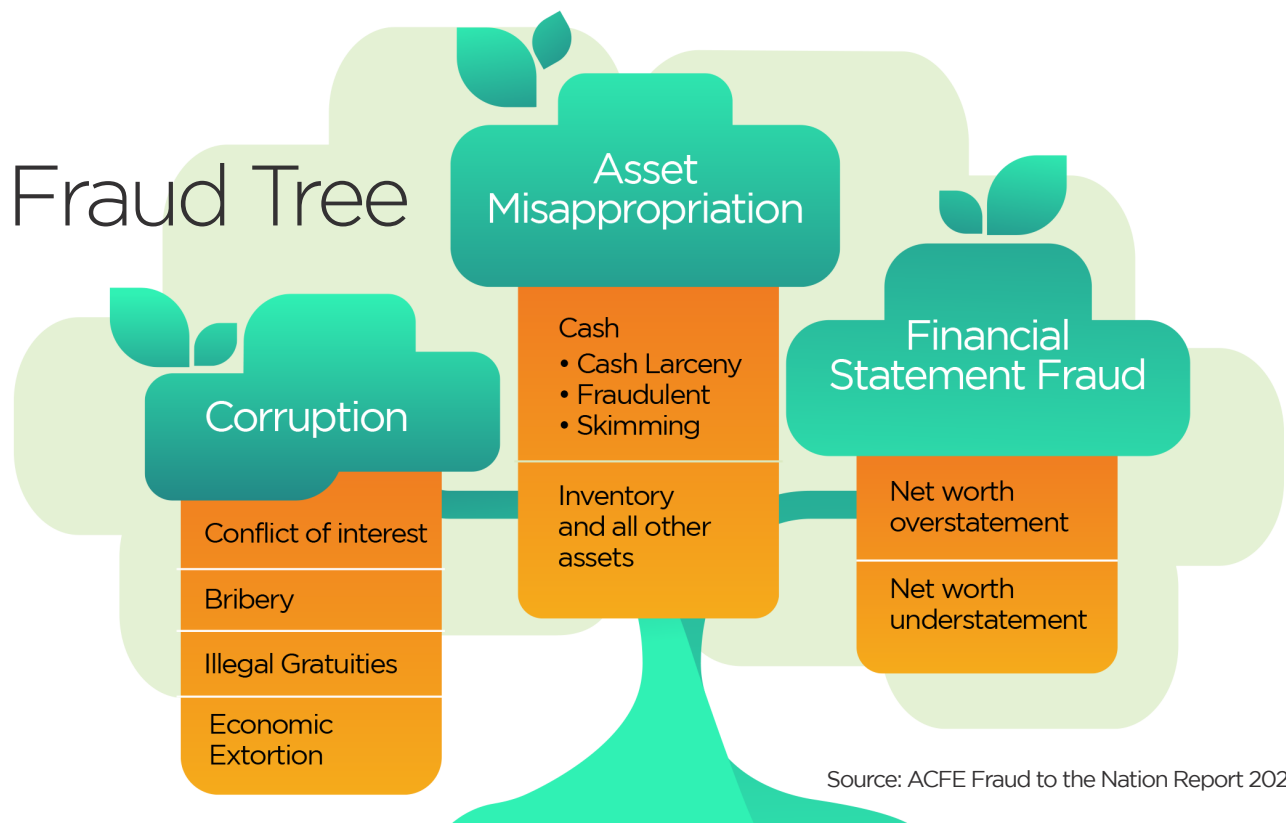
Shyam had recently made few bad investments and was struggling to make ends meet with his current income. These tough times led him to believe that his time and services to the company were not being adequately compensated.

Hence, he strategically decided to cover his

losses through the company's money and manipulate data accordingly to cover his trail. The blind trust and unrestricted access made this embezzlement easier for Shyam.

- Pressure- Bad investments.
- Opportunity- Blind trust and complete access.
- Rationalization- Not enough compensation for his years of service.

02



ACFE Fraud Tree

Corruption

- A scheme in which an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit.
- 50% of the cases with a median loss of \$ 150000 constitutes corruption

Asset Misappropriation

- A scheme in which an employee steals or misuses the employing organization's resources.
- It is the most commonly but least costly
- 86% of the cases with a median loss of \$ 100000 constitutes Asset misappropriation

Financial Statement Fraud

- A scheme in which an employee intentionally causes a misstatement or omission of material information in the organization's financial reports.
- They are the least common but most costly
- 9% of the cases with a median loss of \$ 593000 lacs constitutes financial statement frauds

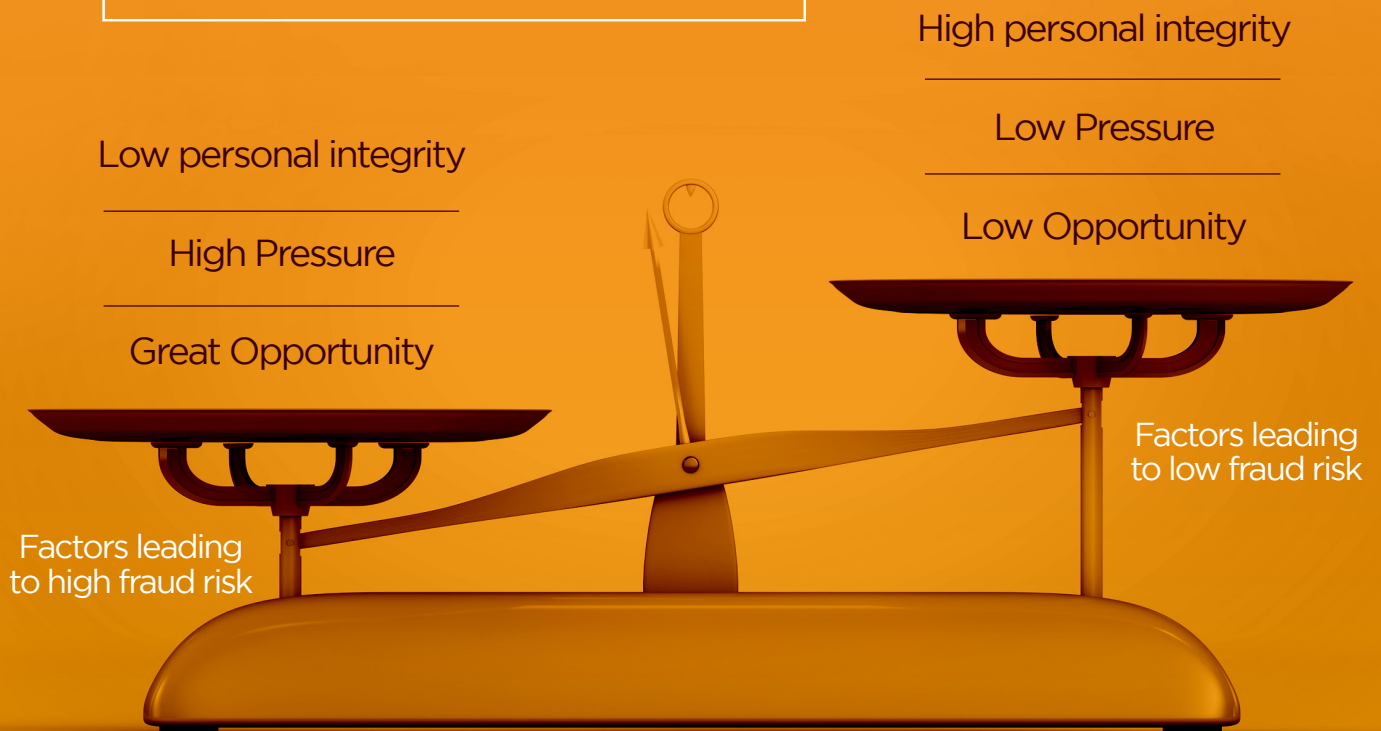
“There is no right way to do the wrong thing”

-Christopher Kent Gilbert

03

Fraud Scale

The fraud scale turns the elements of the fraud triangle into a balancing scale. However, unlike fraud triangle, fraud scale includes integrity instead of rationalization. Integrity can be easily observed in the person's decision making, in the form of their commitment to ethical behavior. A person with integrity does the right thing, even behind closed doors. In the above example, if Shyam had high integrity, his conscience wouldn't have allowed him to use company's funds for his own personal gains. The high pressure, presented with an opportunity and low integrity weighed more on him which forced him to commit the fraud.



Theory by Steve Albrecht
and his colleagues

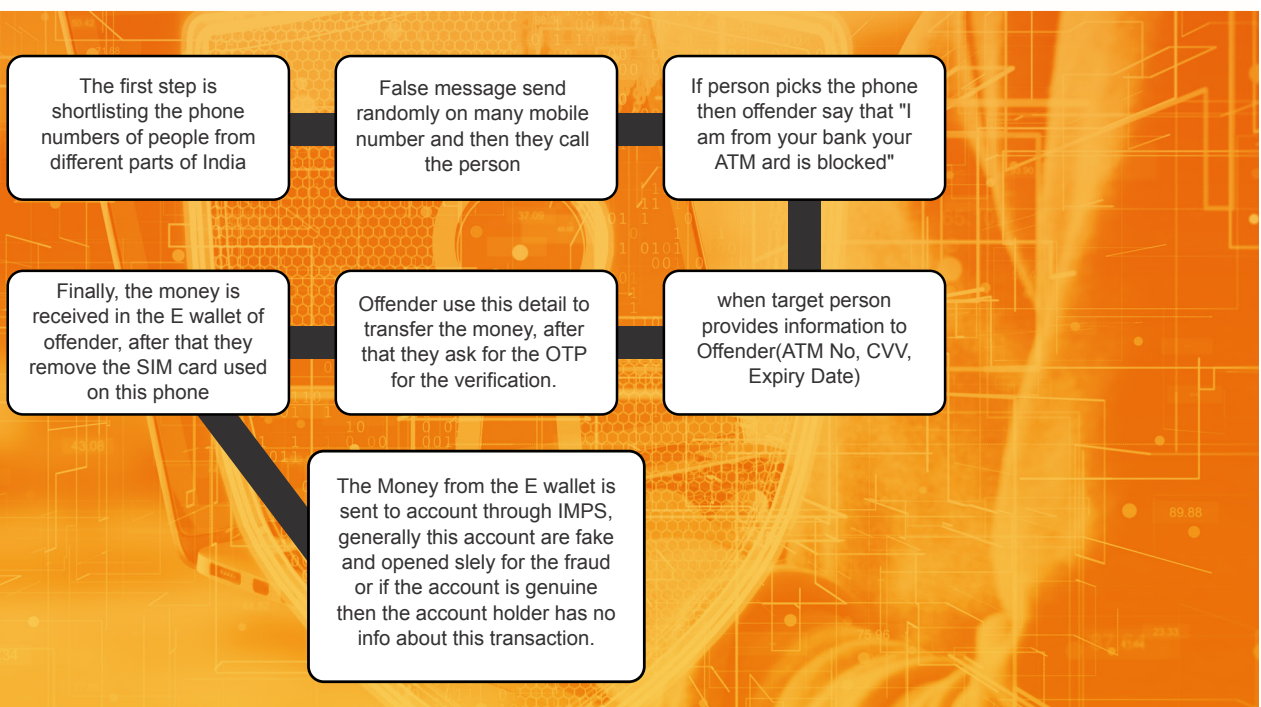
04

Today's Fraud-Vitta VISHING

Vishing also known as voice phishing is a cybercrime that uses the phone to steal personal confidential information from victims, cyber criminals use savvy social engineering tactics to convince victims that they are doing the right things and they end up giving up their private information and access to bank accounts, Often the caller will pretend to be calling from the government, tax department, police, or the victim's bank.

A recent and popular example of this type of fraud is Jamtara- a small town in India. The modus operandi here is both interesting and awakening. The most common tactic used is impersonation. They make phone calls posing as bank managers, asking their targets to share bank account and card details on the pretext that their ATM card has been blocked and if not renewed, it will remain inactive.

Beware ! Beware !! Beware !!! Beware !!! Beware!!!!



Learnings from Fraud-vitta

Be very suspicious of any caller who asks you to share login information over the phone. If a caller asks you to provide account data or personally identifiable information, refuse to do so and report to the concerned authority Bank will never call you requesting you to change user ID, passwords, or network settings. Any caller who makes this type of request is probably a scammer. Refuse the request



Forensics | Risk Advisory | Taxation | Process Management

 +91 9891536969

 info@addvals.in

 www.addvals.in

GURUGRAM | DELHI | KOLKATA | VADODARA | BANGALORE

DISCLAIMER

The document you received is intended for information purposes only . The sender neither gives any guarantee nor assumes any liability (of whatever content or nature) for the information contained in the document directly or indirectly referred to by links or references named in the document. Information mentioned in the document might be protected by copyright and reproduction of such information shall only be allowed with the sender's permission.