FRAUD PREVENTION ANALYSIS

Akinwale Akintayo

https://www.credly.com/badges/9665a811-a57f-4586-801d-235799b330f5/linked_in_profile

https://www.udemy.com/certificate/UC-f212able-ecc8-410f-b8cc-6bb23e6894e/

WHAT IS FRAUD?

In the dynamic landscape of business, the challenges of risk and fraud loom large, necessitating robust preventive measures. To ensure operational resilience and safeguard stakeholder interests, organizations must adopt proactive strategies against risk and fraud. This overview delves into the essence of risk and fraud prevention, offering insights into the definition of fraud and its diverse manifestations.

Definition of Fraud: Fraud is a purposeful and deceptive activity undertaken with the intention of securing financial gain or inflicting loss upon another party. It entails acts of dishonesty, the distortion of facts, or engaging in deceitful conduct. The repercussions of fraudulent activities can be profound, impacting both individuals and organizations through financial losses, reputational harm, and legal ramifications.

What Is Fraud? Definition, Types, and Consequences (investopedia.com)

TYPES OF FRUAD

FINANCIAL FRAUD

Involves manipulating financial transactions or statements.

IDENTITY THEFT

Unauthorized use of personal information for financial gain.

INSURANCE FRAUD

Falsifying or exaggerating insurance claims.

CYBER FRAUD

Illegitimate activities conducted online, such as phishing or hacking.

DATA AND ANALYSIS

As per data from ExpertMarket, the global losses attributed to fraud in e-commerce transactions surpassed US$41 billion in 2022 alone. Additionally, chargeback fraud incurred sellers a substantial loss of over $20 billion the previous year. The combined direct and indirect costs associated with chargebacks are anticipated to escalate to US$117.47 billion by 2023, with a notable 86% of chargebacks identified as probable instances of 'friendly fraud.'

RECENT FRAUD MEDIUMS

POS RECEIPTS

Opt for digital receipts for certain sensitive card information when they are no longer in use.

BANK

Legitimate financial institutions, including banks, do not solicit confidential information through text messages or phone calls. If uncertain about a caller's authenticity, it is advisable to end the call and promptly inform your bank.

OTP/PASSWORD

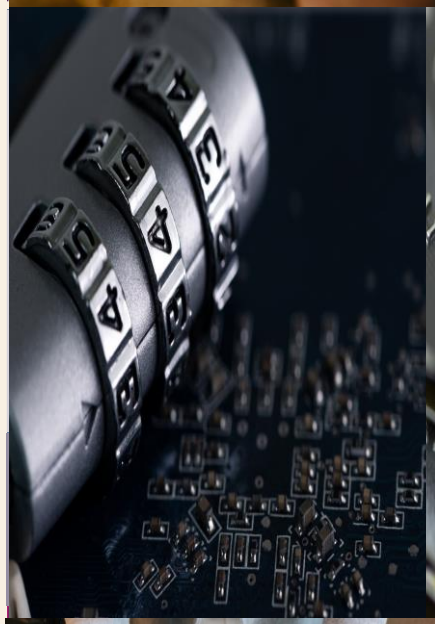
Storing your passwords and other credentials on your phone raises the risk of falling victim to identity fraud. Avoid saving your credentials and make sure to implement Multi-Factor Authentication (MFA) on all your essential accounts to minimize the likelihood of hacking incidents.

CARD/PHONE

Losing your card or phone shouldn't equate to losing your funds. If your card or phone is lost, it's crucial to contact your bank promptly.

ISW_x_International_Fraud_Awareness(2022)





OTHER FRAUD METHODS AND TECHNIQUES

FORGERY:

Faking documents or signatures.

Phishing:

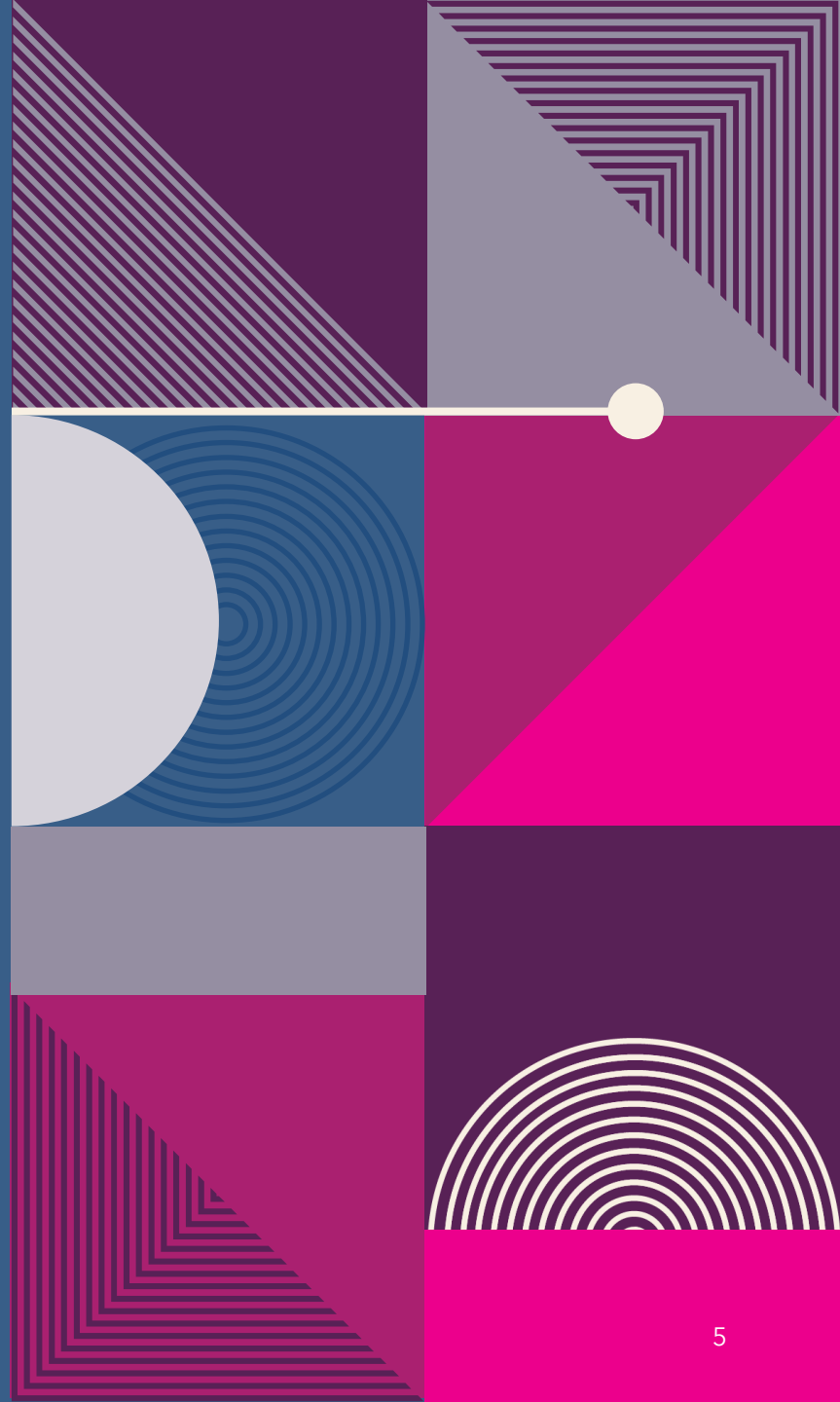
Obtaining sensitive information through deceptive emails.

Credit Card Fraud:

Acquiring confidential information through deceitful means

Insider Fraud:

Deceptive actions by individuals within an organization.



CASE STUDY 1: CAPITAL ONE DATA BREACH (2019)

In July 2019, Capital One announced that it had fallen victim to a data breach, affecting approximately 100 million individuals in the United States and around 6 million in Canada. The breach occurred due to a vulnerability in the bank's web application firewall, exploited by a hacker.

The compromised information included names, addresses, credit scores, and social security numbers of customers and applicants. Additionally, the breach exposed credit card application data, including credit scores, credit limits, balances, and payment history. Thankfully, no credit card numbers or login credentials were compromised.

Key Points:

(i)Response and Investigation (iv) Legal Consequences

(ii) Impact on Customers (v) Improvements in Security Measures

(iii) Regulatory Scrutiny

Whittaker, Z. (2019, July 29). The Inevitability of Capital One's Breach: A Consequence of Inaction Post-Equifax. TechCrunch. [Online] Available at: https://techcrunch.com/2019/07/29/capital-one-breach-was-inevitable/

CASE STUDY 2:
THE HUSHPUPPI CYBERCRIME SAGA

In June 2020, Hushpuppi was arrested by Dubai police for alleged involvement in a global cybercrime conspiracy. The charges against him included money laundering, wire fraud, and business email compromise schemes that targeted individuals, corporations, and government entities.

Hushpuppi and his associates were accused of orchestrating sophisticated scams, including fraudulent schemes that involved compromising business emails to redirect payments. The group reportedly defrauded individuals and organizations of significant sums of money.

Conclusion: The Hushpuppi cybercrime saga serves as a stark reminder of the challenges posed by cybercriminals operating on a global scale. It underscores the importance of international cooperation among law enforcement agencies to tackle cyber threats and financial fraud in an increasingly interconnected world.

Hushpuppi: Notorious Nigerian fraudster jailed for 11 years in US - BBC News

IMPACT AND CONSEQUENCES

Fraud has far-reaching consequences on individuals, businesses, and economies:

- **Financial Loss:** Direct impact on monetary assets and resources.
- **Reputation Damage:** Loss of trust and credibility in the eyes of stakeholders.
- **Legal Ramifications:** Fraudulent activities may lead to legal actions and penalties.
- **Operational Disruption:** Disruption of normal business operations and processes.

HOW TO PREVENT THESE FRAUDS

ADVANCED TECHNOLOGY

Implement robust cybersecurity measures to protect against cyber fraud.

WHISTLEBLOWER MECHANISMS

Establish confidential reporting channels for employees to report concerns.

EMPLOYEE TRAINING

Educate employees on recognizing and reporting suspicious activities.

IDENTITY VERIFICATION

Employ stringent identity verification processes for customers and employees.

REGULAR AUDITS

Conduct regular internal and external audits to detect anomalies

STRATEGIC PARTNERSHIP

Collaborate with law enforcement and industry partners to share intelligence on emerging fraud trends

INDICATORS TO DETECT OR IDENTIFY FRAUDULENT TRANSACTIONS OR ACTIVITIES

Unusual Purchase Timing:
Transactions made during non-business hours or on holidays.
Frequent purchases during times when the account holder is typically inactive.

Unusual Account Activity:
1.Rapid, unexpected changes in transaction patterns.
2.Frequent transactions at odd hours or from unusual locations.

Large or Unusual Transactions:
1.Abnormally large transactions that deviate from typical behavior.
2.Transactions to unfamiliar or high-risk locations.

Unexplained Account Access:
1.Multiple logins from different geographic locations in a short time.
2.Login attempts with incorrect passwords or security credentials.

Sudden Increase in Chargebacks:
1.A surge in customer disputes and chargebacks may indicate potential fraud.
2.Multiple chargebacks on a single account within a short timeframe.

Irregular Purchase Patterns:
1.Purchases that differ significantly from the usual spending habits.
2.Sequential or repetitive transactions in a short period.

Inconsistencies in Customer Information:
1.Mismatch between provided information and validation data.
2.Frequent changes in customer details without proper verification.

THANK YOU

Akinwale Akintayo
akinogbo001@gmail.com
www.academsolutions@mail.com