CONF42 - Incident Management Conference

AI-Powered Detection and Monitoring of Social Engineering-Driven Fraudulent Payments in Remittance Fintech

Ndubuisi Obirije

0101

The Growing Threat of Social Engineering in Remittance Fintech

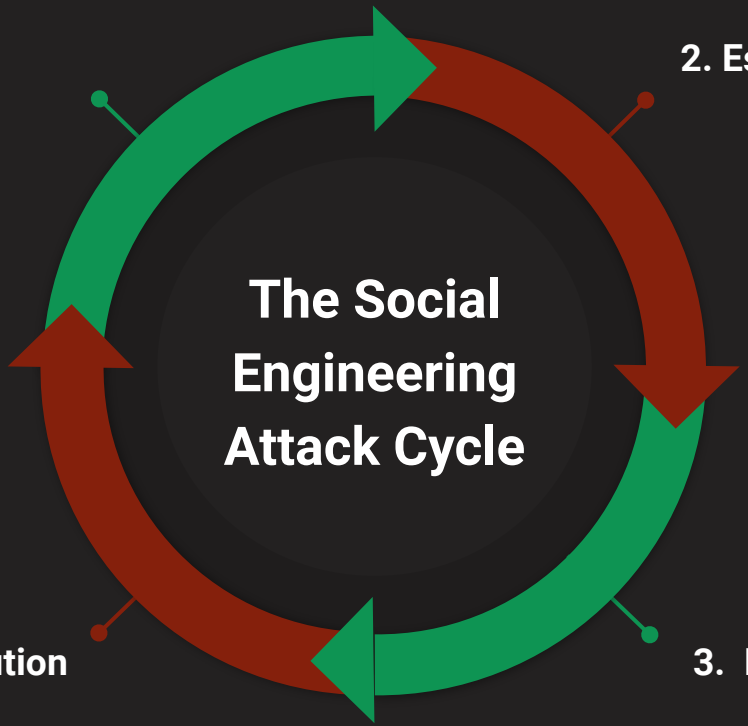
What is Social Engineering ?

Social engineering is the manipulation of individuals to gain access to sensitive information or perform actions that benefit the fraudster.
In the remittance world, this could involve tricking someone into authorizing a payment to a fraudulent account.

What is Social Engineering ?

1. Information gathering

2. Establishing a relationship



3. Exploitation

4. Execution

AI in fintech: Key statistics – part I

The impact of AI in the financial sector is far-reaching, transforming the industry at its core. With the help of statistics, we gain valuable insights into the current state of AI adoption in fintech and glimpse the future of this symbiotic relationship.

AI in Fintech: Key Statistics and Impact – part II

- **Explosive Growth:** The global fintech market is currently worth $340.1 billion, with the AI segment valued at $44.08 billion. AI's share in fintech is expected to reach $50 billion over the next five years, growing at a CAGR of 2.9% *(Fortune Business Insights, Statista)*
- **Widespread Adoption:** 72% of companies utilize AI in at least one business function, with 67% planning to increase spending on data and AI technologies *(McKinsey)*
- **Significant Cost Savings:** AI implementation in identity verification is projected to save banks $900 million in operational costs and reduce digital onboarding processes by 29 million hours *(Accenture)*
- **Improved Customer Service:** AI-powered chatbots and virtual assistants can handle many customer interactions in real-time, reducing the cost of user inquiries by up to 80% *(Juniper Research)*
- **Enhanced Efficiency:** The average time spent per digital onboarding check is expected to decrease by 30% thanks to AI, highlighting its potential to streamline financial operations *(IBM)*

What are Financial Crime and Compliance?

Crime

Financial crime is any activity that involves financial gain but by using illegal means. Even hiding or moving the proceeds of crime is a financial crime.

Compliance

And financial crime compliance is when organizations deploy tactics and strategies to detect, prevent and report these financial crimes or illegal activities.

the value of money laundered in one year globally is in the range of

$800 billion to $2 trillion

Types of Fraud and How AI can Help Prevent

Phishing

an attempt to collect sensitive information, like usernames, passwords, and bank account details, by posing as a trustworthy entity.

How to leverage AI

Advanced machine learning algorithms can analyze patterns in communication and identify phishing attempts. For eg, ML algorithms assess emails for suspicious subject lines or content and alert you for potential phishing attempts.

Identity Theft

involves stealing someone's personal information to commit fraudulent activities. This can range from opening unauthorized accounts to conducting financial transactions in the victim's name.

How to leverage AI

Advanced AI-powered identity verification solutions form a formidable line of defense against identity theft.

Types of Fraud and How AI can Help Prevent

Money Muling

involves individuals who, often unwittingly, become intermediaries in illegal financial transactions. Criminals recruit these individuals to move illicit funds through their bank accounts, exploiting them as a means to obscure the true origins of the money.

Document Forgery

involves creating or altering official documents. Fraudsters use sophisticated techniques to produce counterfeit identification, bank statements, and other critical documents.

Account Takeover

a malicious practice wherein cybercriminals gain unauthorized access to a user's online accounts, exploiting personal information for nefarious purposes.

DeepFake Fraud

a rapidly evolving form of cybercrime that leverages artificial intelligence (AI) to manipulate or mine data science and generate realistic-looking multimedia content, often using facial or voice synthesis technology.

Case study

80% accuracy

in flagging social engineering-driven transactions

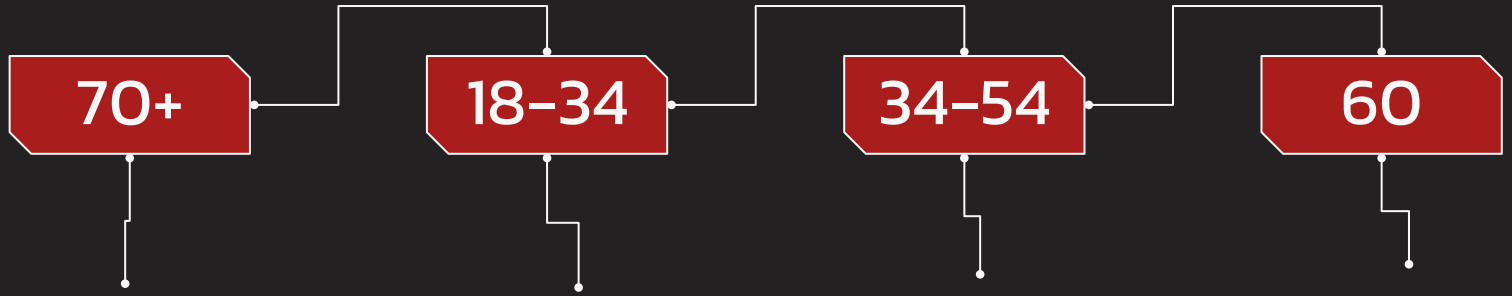
over $1 million

Identified and prevented in fraudulent transactions in the few period this was deployed

Significant reduction in false positives and investigation time

afriex

Here's a breakdown of common victims:



Older Adults (70+)

Their t**rusting nature** and **potential lack of familiarity** with technology can make them susceptible to exploitation.

Younger Adults

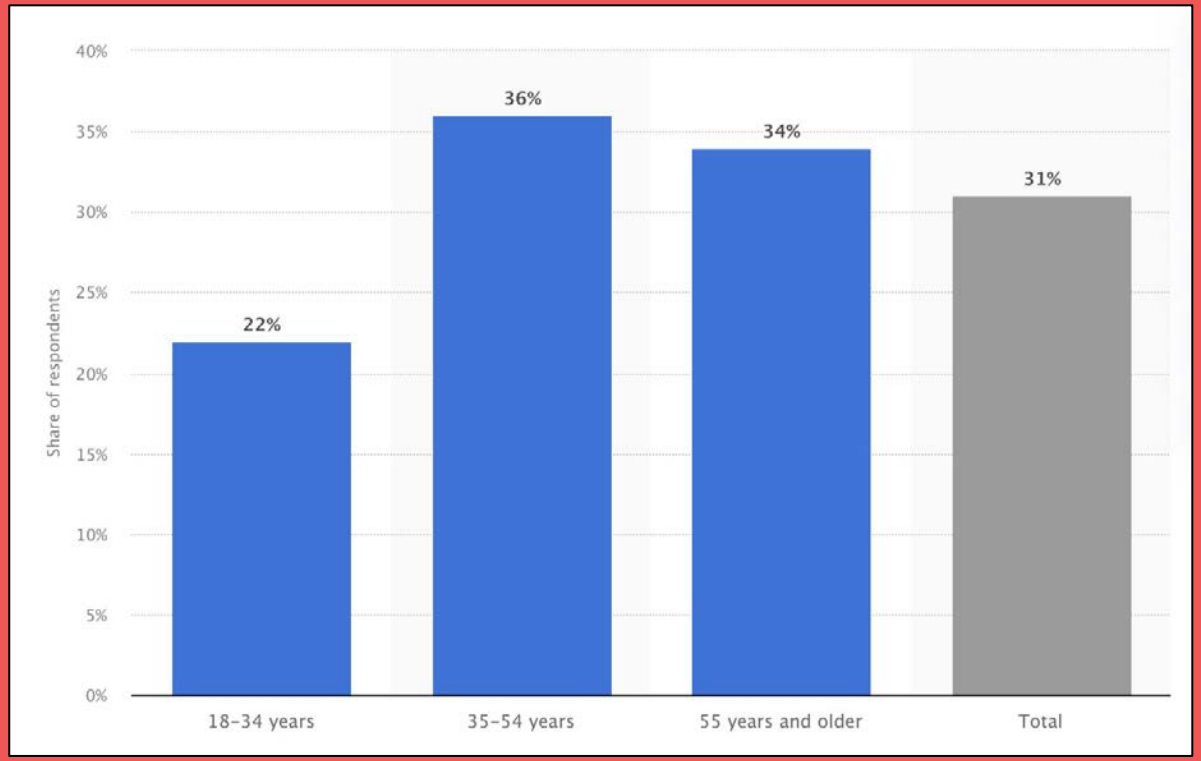
Their **increased digital presence** can make them attractive targets for criminals.

Adults

This may be due to their **higher levels of online activity** and **access to financial resources**.

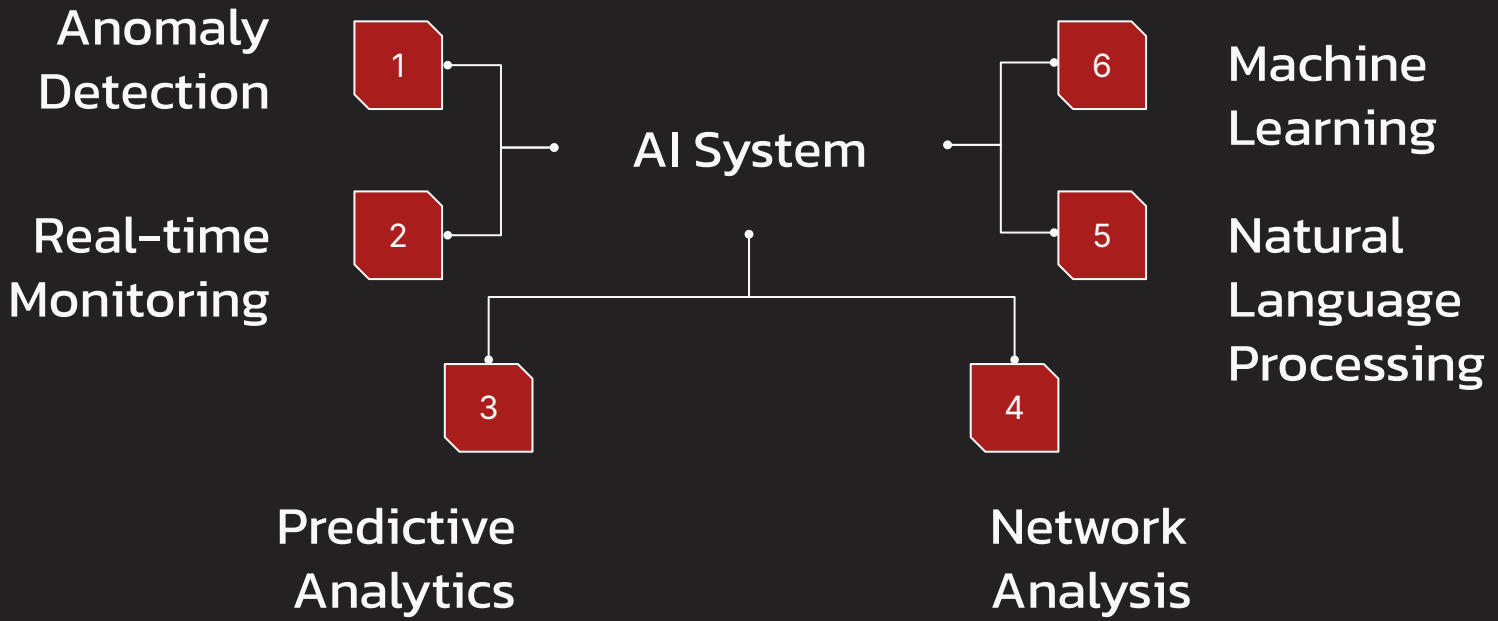
Older adults

In the U.S., this group accounted for the highest amount of financial losses from reported cybercrime



A September 2023 survey of American adults found that three in 10 respondents had experienced financial fraud or cybercrime. Individuals between 35 and 54 years were more often targeted by financial cybercrime, with 36 percent stating so. Among the younger generation, individuals between 18 and 34 years, this share was lower, 22 percent.

AI Solutions to Combat Financial Crime



Key Takeaways:

- **No one is immune**: Financial criminals are opportunistic and target individuals across all age groups.
- **Vulnerabilities vary:** Different age groups are more susceptible to particular types of fraud, often due to factors like digital literacy, financial knowledge, and social trust.
- **Awareness and education**: Empowering individuals of all ages with knowledge about common scams and safe online practices is crucial for prevention.
- **Targeted protection**: Financial institutions and authorities should develop and implement age-specific fraud prevention strategies to address the unique needs and vulnerabilities of different age groups.

Thank you!

Ndubuisi John Obirije
CTO, Afriex

Email: john@afriex.co
https://afriexapp.com