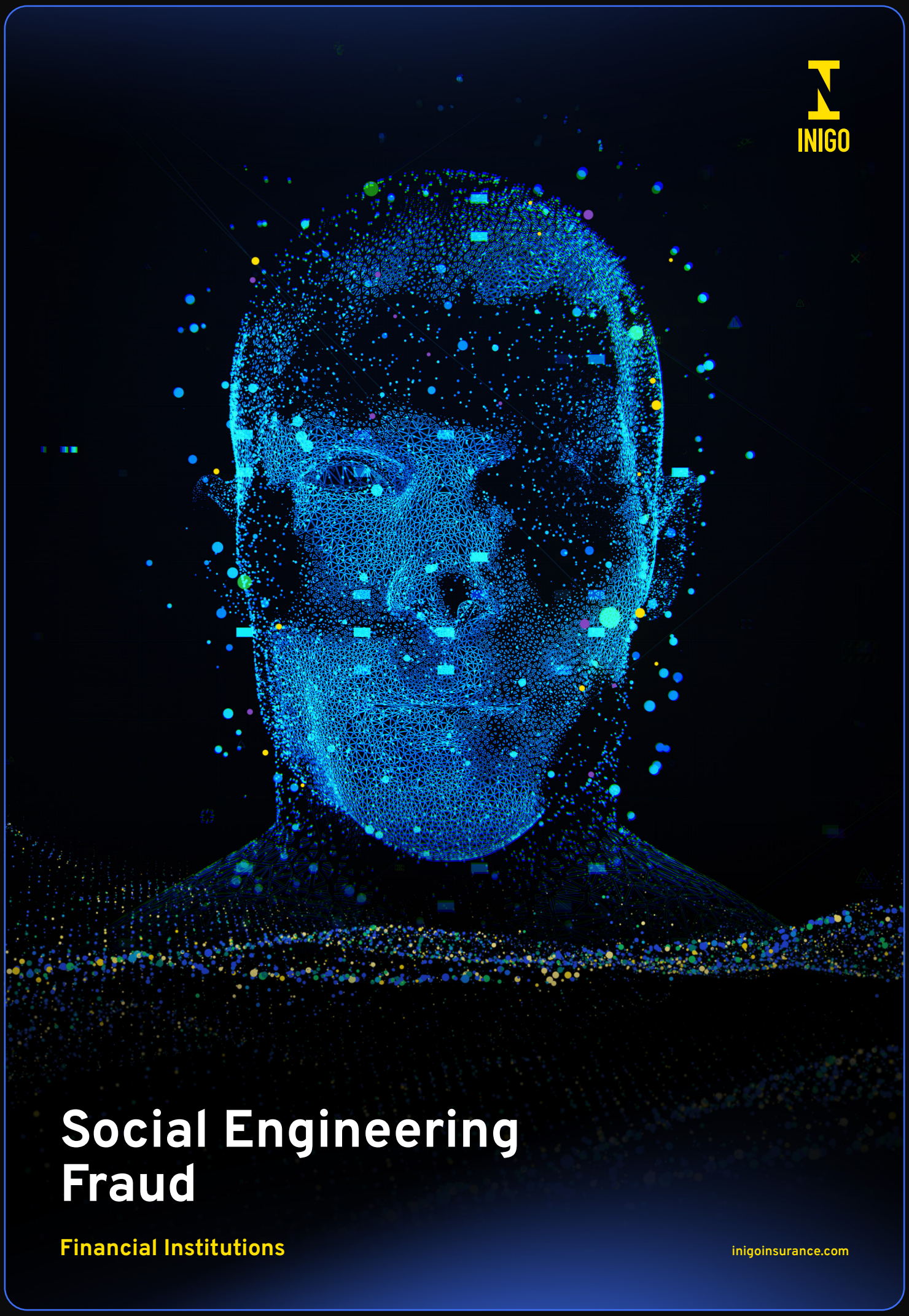
INIGO



Social Engineering Fraud

Financial Institutions

inigoinsurance.com

Introduction

In 2023, global losses from fraud scams and bank fraud schemes amounted to

an estimated $485.6 billion[1]

Among these, social engineering fraud has emerged as a significant threat in the digital age, exploiting human psychology to manipulate individuals into revealing sensitive information or to perform actions that compromise security.

State-sponsored groups like the Lazarus Group have used this tactic in geopolitics, recently stealing $1.5 billion from the crypto exchange Bybit.

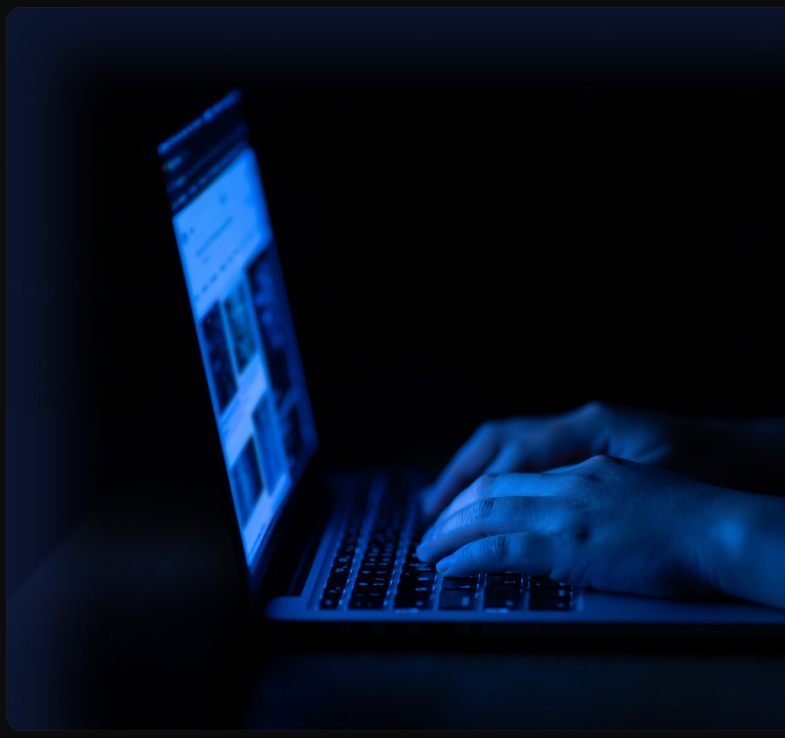
By understanding the methods employed by fraudsters and implementing effective mitigation strategies, businesses and individuals can better protect themselves against these sophisticated attacks. This article explores the various risks associated with social engineering fraud, provides case studies, highlights emerging threats, and explains how Inigo can help.

Social Engineering Risks, Evolution and Case Studies

Let's start by understanding what social engineering fraud is. This type of fraud involves criminals pretending to be trusted individuals to deceive their victims.

They exploit trust to trick people into revealing sensitive information or handing over money. These attackers use strong social skills to manipulate their targets, hence the term 'social engineering fraud'. This can happen through phone calls, emails, or chat apps, often with a sense of urgency that encourages quick compliance and bypassing standard verification and safety procedures.

In a business context, this might involve someone posing as a director or a client who urgently needs funds transferred. As awareness of these scams grows, criminals have diversified their methods, leading to many types of social engineering attacks, including:



- Investment Scams
- Phishing
- Spear Phishing
- Whaling

Fraud and social engineering scams are more common than you might think.

- According to the UK Government's Cyber Security Breaches Survey 2024, **58% of large businesses have experienced a cyber-attack in the last 12 months**, with phishing being the most common (84% of businesses).
- YouGov estimates that UK businesses have lost approximately **GBP 7.78 million due to cybercrimes**, with **91%** of large businesses experiencing a phishing attack, **80%** impersonation fraud, **40%** malware attack, and **14%** unauthorised access by people within the organisation[2].

One of the most prominent social engineering threats is Business Email Compromise (BEC), where fraudsters impersonate senior executives or trusted suppliers to request payments to fraudulent accounts. BEC scams are particularly dangerous due to their low-tech nature and high success rate. In 2023 alone, global losses from BEC fraud reached $6.7 billion[3].

These scams often target high-value transactions, such as real estate deals, where the stakes—and potential payouts—are significantly higher[3].

We are now in an era where fraud has become industrialised. Advances in technology have turned fraud into a profit-making machine, enabling criminals to enhance attacks globally. According to the GBG Global Fraud Report 2024, 79% of companies have seen a significant increase in the sophistication of fraud attempts in the past 12 months[4].

Notable Case Studies:

Bangladesh Bank Heist (2016)

Hackers used phishing emails to steal credentials, leading to an $81 million theft.

Toyota (2019)

A social engineering attack led to a $37 million loss when attackers convinced a finance executive to change bank account details for a wire transfer.

ByBit (2025)

Hackers from the Lazarus Group exploited a free storage software product used by Bybit to move Ethereum, using phishing attacks to gain access and install malware. The hackers stole nearly $1.5 billion.

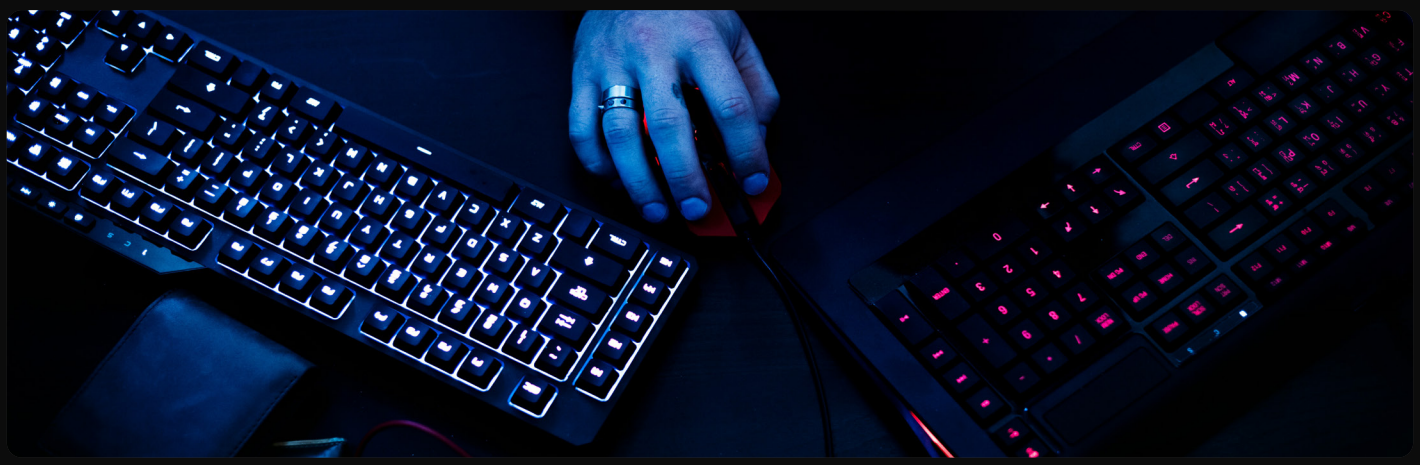
Advancements in Social Engineering Fraud

As financial institutions bolster their defences against fraud, attackers are continuously evolving their tactics with increasing sophistication. This evolution is largely driven by rapid advancements in technology, particularly the widespread adoption of artificial intelligence (AI) over the past three years. AI has become a powerful tool for fraudsters, enabling them to craft more convincing and targeted social engineering attacks that exploit human vulnerabilities and institutional trust.

AI has significantly expanded the threat landscape. It allows fraudsters to automate the identification of system vulnerabilities, generate deepfakes, and create fake identities. Cybercrime groups like the GXC Team have even developed tools such as ‘googleXcoder’ to generate fraudulent invoices for BEC scams. These developments highlight the growing use of AI to enhance the realism and scale of social engineering attacks.

Key risks include the automation of phishing campaigns, the use of AI-generated media to bypass security, and the exploitation of vast data sets to tailor attacks to specific targets.

While AI introduces substantial risks, it also offers opportunities to improve fraud detection and compliance. Financial institutions must remain vigilant, investing in advanced AI-driven security measures and employee training to stay ahead of these evolving threats.



Mitigating Social Engineering Fraud in the future

Mitigating social engineering fraud requires a strategic blend of advanced technology, rigorous employee training, and comprehensive security protocols. As financial crime becomes more sophisticated, organizations can leverage AI and machine learning to bolster fraud prevention while fostering a security-conscious culture among their workforces.

Leveraging AI for Fraud Prevention[1]

Financial institutions are increasingly relying on AI-driven solutions to combat fraud, with 58% of organizations using AI to examine beneficial ownership information and 56% deploying AI-powered financial crime analyst co-pilots. At its core, AI is pattern detection and generation technology, and by that definition, it can be incredibly powerful in transaction monitoring – spotting the outliers and suspicious transactions more easily, and efficiently, than a human would. This reduces remediation times and improves efficiency in fast payment systems. Additionally, predictive analytics allow institutions to anticipate fraud risks by analysing historical transaction data, while AI techniques (such as Natural Language Processing) help detect fraudulent communications in emails, chat logs, and social media.

Generative AI has gained traction, with 55% of institutions using it for alert explanation/narrative generation, and 54% applying it to compile and analyse customer risk profiles. Furthermore, blockchain technology is being integrated with AI to enhance security and transparency, ensuring fraud prevention through decentralized and immutable ledgers. AI-powered risk scoring enables businesses to prioritize investigations effectively, assigning risk levels to transactions and customers based on behavioural patterns.

Strengthening Employee Training & Security Culture

Despite technological advancements, human awareness remains a critical defence against fraud. A survey by YouGov found that 35% of businesses reported scams involving email or online impersonation, while malware attacks affected 17% of businesses[2]. Regular phishing simulations and cybersecurity training empower employees to recognize and report suspicious activities, minimizing vulnerabilities to social engineering attacks. Security protocols such as multi-factor authentication (MFA), encrypted communications, and restricted administrative rights are essential safeguards[1] when it comes to cyber security. The proportion of businesses using up-to-date malware protection increased from 76% to 83% between 2023 and 2024, while network firewall adoption grew from 66% to 75%[2]. Companies must also strengthen third-party risk management, ensuring vendors comply with stringent security standards to prevent potential breaches.

Continuous Improvement & Innovation

Staying ahead of fraudsters requires continuous security updates and investment in emerging technologies. AI adoption in anti-financial crime programs is expected to rise, with most organizations planning to increase spending on machine learning and AI-driven risk assessment tools.

By combining AI-driven fraud detection with employee awareness and strong cybersecurity protocols, businesses can significantly reduce their exposure to social engineering fraud and maintain trust in financial transactions.

How Inigo's ICE Product can help

Having the correct preventative and mitigation measures in place is, of course, imperative but sometimes these attacks will still get through the defences. In a world where sophistication of attacks is heightened, it has never been more crucial for businesses to protect their balance sheets against these attacks with insurance. The percentage of businesses with cyber insurance increased from 37% to 43% from 2023 to 2024, reflecting a growing emphasis on financial risk protection[2].

The need for appropriate and modern types of insurance has never been higher and at Inigo, we believe the US bond market is underserved by the traditional bond policies currently on offer. Financial Crime seems to take a backseat in priority to the liability covers and as such has not benefited from an up-to-date product to suit the threats of the modern world. At Inigo, we strive to be innovative whilst at the same time recognising the importance of longstanding relationships when it comes to insurance. It is with these two things in mind that we have created the ICE policy.

The ICE policy is an excess DIC/DIL policy designed to sit excess of traditional US bond policies, providing top up cover for the standard Crime clauses, whilst dropping down to cover social engineering fraud losses and digital asset losses from the primary or in excess of any sub-limits already provided for. We will underwrite this exposure and provide feedback as to controls if necessary.

Additional Coverages

- Ground up and full limit social engineering cover
- Optional Digital Asset cover from primary
- Excess limit for the standard bond clauses

Benefits

- DIC/DIL excess layer with broader cover to include social engineering fraud cover for the full layer limit
- Social engineering cover is untested/unverified
- Optional inclusion of Digital Asset loss
- Allows the insured to retain consistency of primary carrier
- Market leading Claims handling
- Insured is able to keep their existing Bond forms without having to take on a completely new policy wording
- Lloyd's security and Capacity – financial strength of AA-
- Global licensing: Lloyd's license provides cover in over 200 territories worldwide

References:

1. 2024-Global-Financial-Crime-Report-Nasdaq-Verafin-20240119
2. Cyber Security Breaches Survey 2024
3. CA_Campaigns_SoFC25_Guide_Digital 2025
4. GBG Global Fraud Report 2024

INIGO