TRENDING TOPICS

ASIA PACIFIC

Liberty Specialty Markets

PROFESSIONAL & FINANCIAL RISKS // CLAIMS // AUSTRALIA

Deepfake social engineering fraud claims are on the rise

Long-established payment verification security methods are more vulnerable than ever due to the convincing nature of deepfake social engineering.


Duis risus felis, mattis eget pretium quis, auctor ac ligula. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Maecenas tincidunt placerat efficitur. Interdum et malesuada fames ac ante ipsum primis in faucibus.
Phasellus massa dolor, sagittis a lorem sit amet, elementum finibus sapien. Nunc pharetra lorem lectus, at posuere dui volutpat sit amet. Nunc vitae tortor lacus. Nulla tempor justo mauris, vitae malesuada mi gravida efficitur. Maecenas elementum sapien ante, id scelerisque mi gravida quis.
Duis risus felis, mattis eget pretium quis, auctor ac ligula. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Maecenas tincidunt placerat efficitur. Interdum et malesuada fames ac ante ipsum primis in faucibus.
Phasellus massa dolor, sagittis a lorem sit amet, elementum finibus sapien. Nunc pharetra lorem lectus, at posuere dui volutpat sit amet. Nunc vitae tortor lacus. Nulla tempor justo mauris, vitae malesuada mi gravida efficitur. Maecenas elementum sapien ante, id scelerisque mi gravida quis.
Aliquam facilisis erat et quam iaculis lobortis. Praesent efficitur eros augue, ac malesuada turpis blandit et. Mauris eros erat, auctor sit amet scelerisque vel, ornare vitae nulla. Nullam tristique magna nulla, imperdiet maximus metus posuere id. Pellentesque vel rutrum turpis, non laoreet mi. Integer fermentum, urna ac lobortis pretium, lacus diam accumsan erat, non ultricies turpis leo auctor tortor.
Curabitur tempus blandit odio, vitae cursus ex vestibulum at. Maecenas porta massa sit amet diam pharetra, vel dignissim erat malesuada. Pellentesque suscipit nulla nec rhoncus maximus. Aenean nisi nulla, tempus et magna nec, facilisis rhoncus lacus. Vestibulum maximus fringilla semper. Nulla iaculis diam eu sem rutrum condimentum. Sed posuere auctor neque.
Curabitur sed sagittis ipsum, nec mattis arcu. Suspendisse efficitur in nisl eget vulputate. Aliquam feugiat et justo at eleifend.
Duis risus felis, mattis eget pretium quis, auctor ac ligula. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Maecenas tincidunt placerat efficitur. Interdum et malesuada fames ac ante ipsum primis in faucibus.
Phasellus massa dolor, sagittis a lorem sit amet, elementum finibus sapien. Nunc pharetra lorem lectus, at posuere dui volutpat sit amet. Nunc vitae tortor lacus. Nulla tempor justo mauris, vitae malesuada mi gravida efficitur. Maecenas elementum sapien ante, id scelerisque mi gravida quis.
Aliquam facilisis erat et quam iaculis lobortis. Praesent efficitur eros augue, ac malesuada turpis blandit et. Mauris eros erat, auctor sit amet scelerisque vel, ornare vitae nulla. Nullam tristique magna nulla, imperdiet maximus metus posuere id. Pellentesque vel rutrum turpis, non laoreet mi. Integer fermentum, urna ac lobortis pretium, lacus diam accumsan erat, non ultricies turpis leo auctor tortor.
Curabitur tempus blandit odio, vitae cursus ex vestibulum at. Maecenas porta massa sit amet diam pharetra, vel dignissim erat malesuada. Pellentesque suscipit nulla nec rhoncus maximus. Aenean nisi nulla, tempus et magna nec, facilisis rhoncus lacus. Vestibulum maximus fringilla semper. Nulla iaculis diam eu sem rutrum condimentum. Sed po-

Deepfake social engineering fraud is an emerging risk exposure. It exposes vulnerabilities of existing payment verification methods that are in place to prevent long-established forms of social engineering fraud.

What is deepfake social engineering fraud?

- Using deepfake AI technology, fraudsters create convincing false emails that contain audio or visual digital content which is collected from the internet and social media.
- The intent is to build (false) trust or, alternatively create a sense of alarm, which coerces the recipient of the false content to act immediately leading to the divulgence of sensitive information for the purpose of financial fraud.
- To secure (false) trust, deepfake AI technology manipulates audio and visual content collected to impersonate a known figure to the recipient.
- These attacks can take months of planning and research as fraudsters seek to build a robust work product to establish trust with their victim(s).
- Fraudsters often deepfake target company executives, senior leaders, finance managers and human resources staff to gain access to sensitive information.
- The deepfake social engineering email will instruct the recipient to direct or transfer a payment to a bank account under the guise of updated banking details.

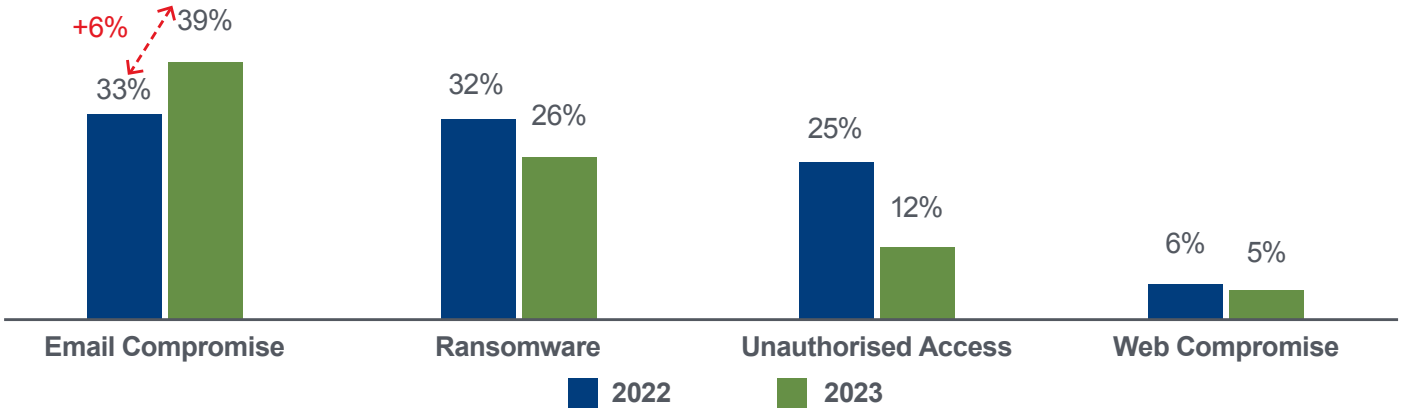
Deepfake technology can be so convincing that it highlights the need for additional layers of security such as cryptographic verification or biometric authentication to prevent unauthorised access and manipulation of business communications.

In 2023, business email compromise – one form of social engineering attack – led the statistics in commercial crime.

A cyber threat landscape report recently produced by Kroll and Liberty Mutual reported comparison data for 2022 and 2023 by threat incident. The data reflects a sharp rise in business email compromise demonstrating that it continues to be a highly profitable model for fraudsters and remains a prominent financial crime risk exposure for companies globally.

Threat Incident Types

Year-on-Year Comparison: Most Common Threat Incident Types 2022 Vs. 2023



Kroll continued to see email compromise dominate as an incident type in Q4. As expected after a lull in Q3, ransomware rebounded during the fourth quarter, accounting for 23% of all cases.

Liberty Mutual INSURANCE

KROLL

Case Studies

The following deepfake social engineering case studies illustrate how deepfake technology can be leveraged by threat actors in social engineering attacks to deceive recipients and facilitate financial fraud outperforming robust internal verification processes.

01 Social engineering fraud with deepfake audio recording

A funds management company acting on behalf of a client found itself a victim of a sophisticated crime involving deepfake AI technology.

The company was working on a significant business transaction that involved a substantial transfer of funds. The recipient being the custodian of the funds who had a longstanding and trusted relationship with the company, and was very familiar with the company's internal accounts team.

A threat actor discovered the company's integrated phone system, which converted voicemails into digital email audio messages. Utilising AI technology to manipulate voice memos and telephone calls, the threat actor was able to impersonate the custodian, which enabled them to set the following events in motion:

The threat actor created a deepfake audio recording of the custodian using AI technology.

The company received an email supposedly 'the custodian', requesting the funds to be split between two accounts.

To add an extra layer of legitimacy, the accounts team received a phone call from 'the custodian', confirming the request and providing the necessary bank account details.

With the account details seemingly verified, the company proceeded to carry out the transfer as instructed.

Days later, the (real) custodian contacted the company, expressing concern the funds had not arrived. An extensive investigation revealed the email instructing the company to split the transfer had fallen victim to a business email compromise, and the threat actor had simulated their voice during the verification process.

In response, the company has taken robust measures to enhance its security protocols, heightening awareness of combined email and audio-based fraud, and implementing safeguards to combat the rising prevalence of deepfake crimes.

Case Studies

02 Social engineering fraud with deepfake call verification interception

A financial services company acting for a client in a transaction found itself a target of fraud that involved deepfake AI technology.

As part of the transaction process, the company's Account Manager sent the client (who was someone well known to the Account Manager) forms to complete which included requesting bank account details for the transfer of funds.

Unbeknownst to the financial services company and the client, the client had recently fallen victim to a romance scam*, with their personal information and email account being compromised. As a result, the threat actor was able to use AI deepfake technology to impersonate the client in the following transactions:

The Account Manager received the completed forms from the 'client'.

Bank account details were confirmed over the phone, with the voice of the client being impersonated during the verification process.

The Account Manager, having verified the account details, and believing the information provided to be authentic, provided the other side with the relevant bank account details for the transfer of funds to be made.

Threat actor was successful in intercepting the transfer to the account details they provided.

A week later the client contacted the Account Manager seeking an update on the transaction process, as they had not yet been asked to provide bank details. The Account Manager confirmed that the funds had been sent to the account indicated on the forms, to which the client advised they did not complete the forms and had not been contacted by phone to verify.

Upon review of the emails sent by the Account Manager by digital forensic incident response consultants, the fraudulent activity in the alleged client's communications was confirmed, as there was no indication that the company's computer network had not been compromised.

Within nine days of the fraud, the police and bank were able to make a full recovery for the company.

*Romance scam: Threat actor creating a fake persona to mislead a target and feign a romantic connection, with the intention of extorting funds or gaining access to personal information.

Case Studies

03 Social engineering fraud with deepfake video call

A large residential building company found itself the victim of a fraud involving the use of deepfake video deployed with AI technology.

An IT support team member within the company received an email message from the personal email address of a key staff member within Accounts Payable, who advised they were experiencing an IT issue that was preventing them from accessing any of their work devices.

After responding to the email, the IT support team member received a FaceTime video call from the affected individual seeking more information.

Whilst on the phone, the individual expressed that there was a large payment outstanding which required actioning straight away.

As the individual was known to the IT support team member, they proceeded to reset all user account passwords and multifactor devices.

The following week, the IT support team received another call from the affected individual, who stated they had just returned from annual leave and were unable to access their account.

It was later identified that the organisation had been the target of a sophisticated deepfake social engineering campaign, which had collected information from the company's LinkedIn page and social media pages of individuals to initiate their attack while their target was on annual leave.

As the threat actor had been successful in requesting passwords to be reset and shared over the phone, they were able to access the Accounts Payable mailbox, intercepting and manipulating multiple invoices and inserting fraudulent bank account details.

In order to enforce the changes to the bank account details, the fraudster utilised further video-calling functionality with Microsoft Teams to call additional staff members who were able to update invoicing systems with new bank account details.

Our Claims Value Proposition is demonstrated through our incident response framework and claims approach

Experienced claims specialists financially empowered with local authority to manage complex claims with transparency and agility

We partner with our clients to provide value-added support when they need it the most

Pre-loss assistance to clients – through a claims simulation workshop before an incident occurs; 'stress testing' social engineering verification processes: 'Claims+'

Post-loss incident response assistance to clients – specialist digital forensic incident advisers engaged from the outset to conduct threat hunt intelligence to investigate the cause and nature of the social engineering fraud quickly at favorable rates (the 'BEC Package')

Dedicated claims recovery specialists who work with our clients to assess recovery avenues and pursue stolen funds

The Liberty Advantage:

An integrated team of underwriters and claims professionals who work together to build long-term relationships

- Proven history of stability throughout volatile market conditions
- Comprehensive and tailored coverage to suit client needs
- Empowered and experienced underwriters who have the ability to provide large limits
- Empowered, experienced and agile claims specialists
- Multinational footprint

Our Policies that provide cover for Social Engineering Fraud

Financial Institutions Insurance

Liberty will pay for any amounts insured under Part A [Professional Liability] or Part C [Crime] of this **Policy** for, arising out of or in any way connected with any actual or alleged **Social Engineering Fraud** is a Sub-Limit of Liability of $[x]. **Social Engineering Fraud** means the misleading of an **Insured** or their **Agent**:

(a) through misrepresentation of a material fact which is relied upon by an **Insured** or their **Agent**; and

(b) which results in the loss of **Property**.

View our Appetite Guide

Meet our Financial Institutions underwriters

Commercial Crime Insurance

Liberty will pay for direct loss of **Money** or **Securities** sustained by an **Insured**, resulting directly from an **Insured Instruction** to transfer, pay or deliver **Money** or **Securities** from a **Transfer Account** as a result of **Social Engineering Fraud** committed by a person purporting to be a **Vendor**, **Client** or **Employee**, provided that such direct loss is **Discovered** during the **Policy Period**.

View the PFR Appetite Guide

Meet our Commercial Crime underwriters

Our coverages withstand deepfake AI social engineering fraud emerging risks

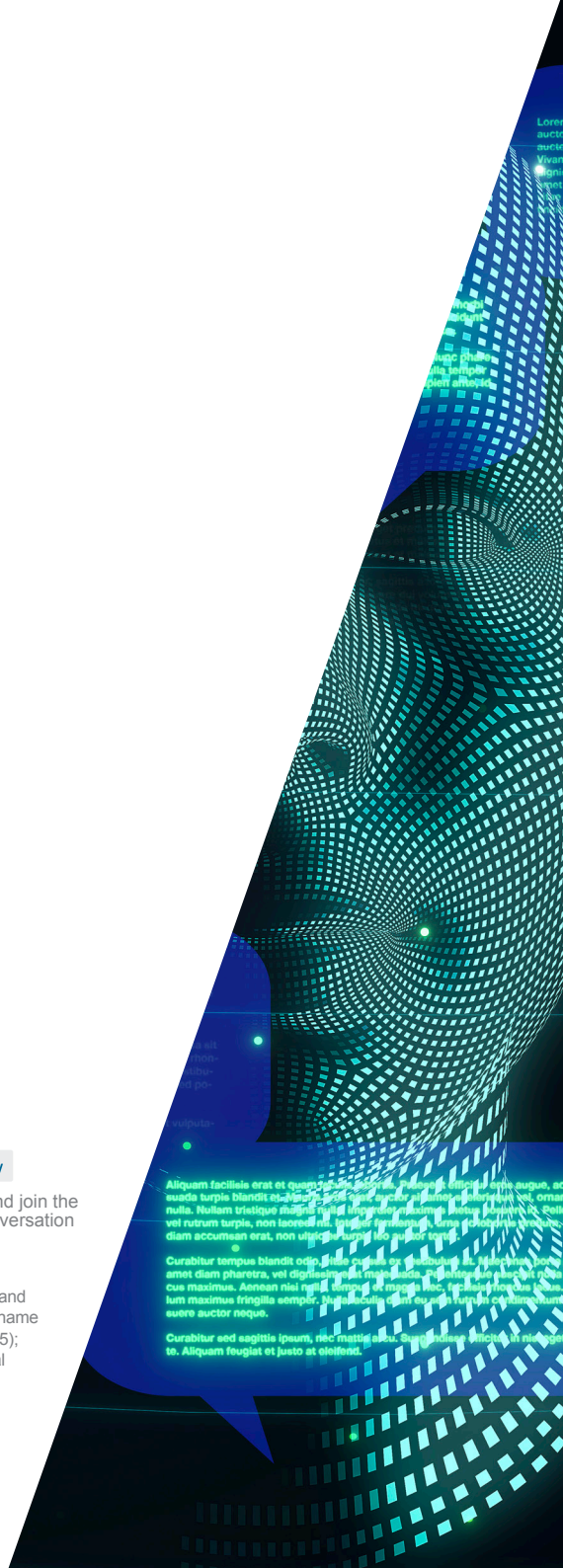
Liberty Specialty Markets

Global reach. Financial strength. Local authority.

Distinct, complex and constantly evolving – every business is as unique as its insurance needs. To confidently progress in the face of risk and uncertainty requires a level of security you can only achieve through working with specialists.

Liberty Specialty Markets offers a breadth of world-class insurance and reinsurance services to brokers and insured clients. We bring value and solutions to more than 26,000 of Asia Pacific's most significant business and government organisations – helping protect what they earn, build and own.

We're part of the global Liberty Mutual Group, a Fortune 100 company that's been in business since 1912 with a Standard and Poor's 'A' rating.



If you have any inquiries, please contact Angela Messih - Senior Claims Specialist & Tech Lead, Professional & Financial Risks

View our office locations

Meet our Professional & Financial Risks claims team

Follow

Connect and join the Liberty conversation

AP0930-04-24