Morrison Cohen

Client Alert | July 17, 2024

Morrison Cohen Cyber Watch: Navigating the Cyber Landscape Safely, Part Two

Top Tips for Protecting Your Business from Deepfake Scams

Digital Fraud on the Rise

Digital fraud comes in many forms, including phishing attacks that target business email systems and scams that attempt to misdirect funds protect via social engineering. These types of attacks have always been a concern for businesses. However, rapidly evolving and increasingly sophisticated technology has made such scams easier to implement and harder to detect. In particular, today's generative artificial intelligence tools, many of which are free to use and available worldwide, allow threat actors to generate and manipulate video and audio files, develop malware and enhance the effectiveness of phishing scams.

Deepfakes Used Against Businesses

In this alert, we want to draw attention specifically to deepfakes—digital manipulations of synthetic media that replace or create a digital representation of a person's likeness, voice or other physical characteristics. The result is a digital representation that appears to be a particular individual's face or voice, but is, in fact, merely an artificial digital image, recording or sound. Some of these tools can create a realistic video that appears to depict a real person speaking, using only a single photo and a speech audio clip. While such technology is still evolving, there are already reports of its successful use, including deepfake sexually explicit videos of singer Taylor Swift, which were recently circulated on social media, and deepfake robocalls which appeared to feature President Joe Biden's voice seemingly discouraging voters from participating in primary elections. Recently, threat actors also succeeded in convincing an employee of a multinational company to send $25 million to an unverified account by using deepfake technology that appeared to show the company's chief financial officer giving directions during a conference call.

The Dangers of Deepfake Scams

In addition to significant financial loss, a business that falls victim to a deepfake scam could also face legal liability, as demonstrated by recent case law. For example, in litigation between parties to a transaction (i.e., a payor and a payee) where funds were wired to a threat actor, courts may apply the Uniform Commercial Code's "imposter rule" and find that the party in the best position to prevent the fraud through the exercise of "reasonable care" should bear the loss.[1] In other cases, where a customer seeks to recover losses incurred when a financial institution authorized a fraudulent withdrawal from the customer's account, courts tend to consider whether the security measures agreed upon to verify payment orders were "commercially reasonable" and whether the financial institution accepted the payment order in "good faith" and in accordance with the security procedures and any

[1] See, e.g., *Arrow Truck Sales, Inc. v. Top Quality Truck & Equip.*, Inc., No. 8:14-CV-2052-T-30TGW, 2015 WL 4936272 (M.D. Fla. Aug. 18, 2015).

written agreement or prior instructions from the customer.[2] Given this potential liability, companies should be vigilant of deepfake scams and ensure that they implement reasonable security measures to combat them.

Detecting Signs of a Deepfake Scam

As part of those security measures, businesses might consider training their employees to detect deepfakes. To date, there are still some telltale signs of a deepfake that might be noticeable, if the employee pays close attention. There may be audio and visual clues to detect when a speaker or video is not who they claim to be – such as strange phrasing or inflection, unnatural pauses in speech, odd facial expressions, unusual body movements, background noise that does not match the speaker's apparent location, visual glitches, and poor audio quality – any of which may indicate a deepfake. Deepfake messages may also include a false sense of urgency in order to spur victims into action, originate from unfamiliar phone numbers or email addresses, or request a change or "update" to previously-used wire instructions. Anything that seems out of the ordinary should be questioned, even if it appears to be coming from a trusted source.

As Protective Measures

Businesses may also want to establish clear protocols (and ensure these are followed) and implement up-to-date technological measures to help detect, and hopefully reduce, their susceptibility to deepfakes. Some approaches can include:

- Prior to wiring money, confirm the wire instructions by calling a known recipient at a known number. Relying on calls from the transferee can be risky, given today's technology, which includes deepfakes and spoofing (i.e., when someone modifies the incoming telephone number when making a call, so as to appear to be someone they are not).
- Consider implementing real-time, face-to-face identification through video conferencing, for example, by having the individual confirming the transfer instructions show state or federally issued identification, like a driver's license or passport. This may add an additional layer of security, since it may be more difficult for threat actors to fake such interactions in real-time or obtain access to the necessary documentation.
- Implement, whenever possible, enhanced authentication methods such as multifactor authentication, biometrics and/or changing security tokens.
- Establish clear company-wide communication protocols for verifying the authenticity of wire requests and instructions received via email, messaging platforms, and phone calls.
- Provide employees with routine and regularly updated training on deepfakes, including what they are, how to detect them, how to respond, and how deepfake technologies are evolving.
- Regularly review and update security measures and protocols to adapt to new threats as they arise over time.

Looking Ahead

It may be difficult to stay ahead of threat actors, especially as novel technology like generative artificial intelligence evolves, but by establishing and routinely updating security measures and controls, and considering the technology currently available to threat actors, businesses can help mitigate the risk of deepfake scams and any accompanying financial loss and legal liability.

[2] See, e.g., Capten Trading Ltd. v. Banco Santander Int'l, No. 17-20264-CIV, 2018 WL 1558272 (S.D. Fla. Mar. 29, 2018); Patco Const. Co. v. People's United Bank, 684 F.3d 197 (1st Cir. 2012).

Key Contacts

Morrison Cohen's Technology, Data & IP team is available to assist clients with any questions regarding potential deepfake issues, including mitigating the effects of deepfake scams and developing and implementing protocols aimed at reducing a business's susceptibility to deepfakes.

Jessica L. Lipson
Partner & Co-Chair

D 212.735.8683
jlipson@morrisoncohen.com

Tess Bonoli
Associate

D 212.735.8728
tbonoli@morrisoncohen.com

Fred H. Perkins
Partner & Co-Chair

D 212.735.8647
fhperkins@morrisoncohen.com

Allison O'Hara
Associate

D 212.735.8807
aohara@morrisoncohen.com

The authors would like to extend their thanks to Morrison Cohen's Chief Information Security Officer, Thomas Catenaccio, for his invaluable contributions to this article.

This document is attorney advertising and is provided for informational purposes only as a service to clients and other friends. This document does not constitute legal advice. Reading or receiving this document does not create an attorney-client relationship, nor should the information in the document be deemed to be provided to you confidentially. Please contact one of our attorneys should you wish to engage Morrison Cohen LLP to represent you, so that an attorney-client relationship may be established between our Firm and you. Prior results do not guarantee a similar outcome.