PUBLICATION

Faking It: Protecting Your Financial Institution Against Deepfakes

Authors: Matthew George White, Alexander Frank Koskey, III
September 11, 2023

Fraudulent activity in the financial industry is nothing new. The techniques employed by fraudsters have ranged from fake check fraud and credit card fraud to identity theft and financial account takeovers. For years, financial institutions have implemented a variety of measures to combat these frauds. Now, thanks to the proliferation of sophisticated and low-cost artificial intelligence (AI) technologies, financial institutions are facing tougher challenges than ever before. One of the biggest challenges facing financial institutions today is that methods commonly used to prevent fraud, such as phone or video calls, are now being used by criminals to perpetrate fraud using deepfakes. This alert will discuss the risks financial institutions are facing from these technologies and provide some practical solutions you should consider as you continue to develop your fraud prevention program.

What are Deepfakes?

Deepfakes is the use of a type of AI called deep learning to create fake images, audio, or videos of events or individuals. Many of you have likely seen this technology in action in recent months. The examples are far-ranging, from videos of Mark Zuckerberg claiming "we own you" and Morgan Freeman explaining that "I am not Morgan Freeman" while providing an overview of synthetic reality, to Jon Snow bemoaning "I'm sorry we wasted your time" and apologizing for the ending of Game of Thrones (explicit). Videos are not the only content being faked. You've also likely seen the viral fabricated images of Pope Francis wearing a floor-length white puffer jacket and fake images of former President Donald Trump's arrest. Complicating matters even more, there are a variety of low-cost tools that can generate deepfake audio content, such as a fraudulent voicemail that was recently used in an attempt to obtain a fraudulent money transfer.

While several of these are "fun" examples of deepfake technology in action, the reality is that the emergence of deepfakes is creating significant risks for financial institutions by adding a heightened level of sophistication to fraud attempts. A deepfake video call could be used to trick an individual into divulging sensitive personal or financial information, or into initiating an unauthorized wire transfer. Similarly, a deepfake voicemail could be used to direct an employee to send money to a fraudster.

Unfortunately, these are not hypothetical examples. There have been numerous reported incidents of precisely these scenarios resulting in substantial losses to companies and financial harm and identity theft to individuals. One such example occurred in 2020 when a bank manager transferred nearly $35 million to fraudsters after receiving what he thought was a voicemail from a company executive but was actually a deepfake. In another recent example, deepfake technology was used to create fake identities that were used to open financial accounts. This type of new account fraud is becoming increasingly common (as are related types of frauds such as "Undead Claims" and "Frankenstein" or "Synthetic" identifies) and is causing significant amounts in losses. Further complicating matters, many financial institutions and their customers rely on verbal communications to verify financial transactions like initiating a wire transfer. If those verbal confirmations cannot be trusted, financial institutions may be forced to find completely new methods of verifying these transactions are legitimate.

Best Practices to Combat Deepfakes

As the number of fraudulent attempts based on deepfake technologies continues to grow, financial institutions must become increasingly vigilant to protect themselves, their employees, and their customers. Several things financial institutions can do to prevent fraud associated with deepfake technologies include:

- Consider these issues as a part of your cybersecurity preparedness plan, working with counsel to develop policies and strategies, and to understand the relevant industry standards.
- Training employees to detect common signs of deepfakes such as unusual skin tones, odd lighting, strange or inconsistent shadows, disproportional sizes of faces and bodies, awkward postures or body movements, inconsistencies in tone or intonation, or lip-synch errors.
- Evaluating AI-based technologies designed to combat fraudulent activities attempted with deepfakes. There are currently several AI solutions available that fight deepfakes by detecting image tampering or facial biometrics to verify and authenticate customers.
- Deploy multifactor authentication across financial institution networks and consider enhanced measures for authentication. Examples could include issuing tokens or physical devices for authentication.
- Consider the use of biometrics (or physical characteristics) for authentication. Biometrics can be a fast and convenient solution to verify customers as this type of data is unique, nontransferable, and hard to fake or steal. However, financial institutions should also be aware of the increasing number of state laws regulating the use of biometrics and ensure they are complying with those regulations.
- Providing customer awareness by teaching customers how to better protect their data.

While AI-based technologies provide some amazing opportunities for both financial institutions and their customers, they also present many significant risks. Among those risks is the increasing availability and low price of deepfake-generating tools. Financial institutions need to ensure they stay up-to-date on developments in these areas and continue to develop, monitor, and improve their fraud prevention programs.

If you have any questions concerning AI, the development of your AI and data governance programs and strategies, your fraud prevention programs, or any aspect of your cybersecurity or privacy programs, please contact Matt White or Alex Koskey, co-chairs of Baker Donelson's Financial Services Cybersecurity and Data Protection Team, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.