WILMERHALE

FBI Warns That Scammers Are Using Deepfakes to Apply for Sensitive Jobs

JULY 1, 2022

On June 28, 2022, the FBI issued a Public Service Announcement (PSA) warning that fraudsters are using deepfakes to impersonate job applicants during online interviews and employing stolen Personally Identifiable Information (PII) to apply for positions. (Deepfakes are realistic synthetic media that are either altered or wholly created by artificial intelligence.)

This type of fraud may be used in an effort to gain access to company networks and to otherwise obtain company data. According to the FBI, the jobs targeted by scammers include remote work or work-from-home jobs in the information technology, computer programming, database, and software fields. "Notably," the PSA from the FBI's Internet Crime Complaint Center said, "some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information." This is a particularly concerning development, given the potential business and legal ramifications to businesses of unauthorized access to PII, under a mosaic of state laws and international protocols.

The FBI reported that the scammers use technology to impersonate another's voice during online interviews. "In these interviews, the actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking," the FBI wrote. "At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually." Furthermore, the complaints indicated that some PII provided for pre-employment background checks was stolen from someone else.

This PSA follows a Private Industry Notification (PIN) the FBI issued in March 2021, warning private companies that "[m]alicious actors almost certainly will leverage synthetic content for cyber and foreign influence operations in the next 12-18 months." The FBI cautioned then that altered media would be used by foreign and criminal actors for social engineering crimes and spearfishing—when a threat actor emails a target from a seemingly trusted sender to trick the recipient into clicking a malicious link or downloading an attachment. The Bureau wrote that Russian- and Chinese-language users were already using falsified profile images to create phony accounts and propagandize and would likely expand their efforts to use synthetic media and deepfakes to attack

the business sector.

The FBI advised that synthetic content could be used in a "newly defined cyber attack vector" called "business identity compromise" (BIC). In a BIC attack, deepfake technology creates "synthetic corporate personas" or imitates existing employees, likely causing "very significant financial and reputational impacts to victim businesses and organizations." BIC is an evolution in business email compromise (BEC) schemes, which occur when a hacker compromises a corporate email account to facilitate fraudulent financial transactions. BEC scams led to financial losses totaling $2.4 billion in 2021, according to an FBI report.

As we wrote in an article assessing the FBI's PIN, "[t]he potential for deepfake technology to create a new category of BIC activities threatens to complicate company authentication protocols" that businesses have put in place to protect their treasury and accounts-payable functions from BEC intrusions.

The FBI's recent PSA validates the Bureau's earlier warnings of the rising dangers to businesses of deepfakes and BIC ruses. To mitigate the risks of deepfakes and these impersonation campaigns, businesses should engage in several best practices:

- **Secure Systems.** Strong cybersecurity protections will help safeguard a company from any cybersecurity incident, including ones where a bad actor attempts to gain system access through deepfake impersonation. As the Cybersecurity and Infrastructure Security Agency recommends in its "Shields Up" program, businesses should consider validating that all remote access network users employ multi-factor authentication, ensuring all software is updated and all known vulnerabilities patched, and that cloud services, if applicable, are using top-of-the-line protections, among other steps. Likewise, firms should consider segregating PII and sensitive data from general-use systems.

- **Prepare and Practice.** Deepfake risk management begins at the top. C-suites should prepare employees for growing cyber threats, like deepfakes, by revising their cyber incident response plans so their workforces know how to identify and respond to disinformation and deceptive media if they arise. Human Resources interviewers should be trained how to detect deepfakes. They should be on the lookout for visual clues of falsity, including visual distortions around pupils and earlobes, indistinct and blurry backgrounds, and random distortions or visual artifacts. Companies should establish clear protocols for when to elevate concerns of BIC campaigns to Chief Information Security Officers (CISOs) and the like.

  Given the increasing likelihood of media manipulation of high-profile corporate leaders, companies should also consider integrating technology into corporate videos that reduces the likelihood that media can later be covertly manipulated. This image provenance technology relies on blockchain technology and metadata to track how a piece of media has been altered over time.

- **Respond.** At the first sign of a deepfake impersonation, businesses should contact counsel to map out a response, investigate where necessary, and coordinate with

regulatory and law enforcement authorities, if appropriate.

WilmerHale is at the forefront of this evolving area of business, law and technology, what we call Disinformation and Deepfakes Risk Management (DDRM). Please click here to view WilmerHale's thought leadership related to disinformation and deepfakes. WilmerHale will continue to follow developments on these matters. To stay updated with our writings on this topic, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.