APR 08
Lauren Ashcraft

# A new kind of AI-generated attack could shift banking strategies

Article

**The news: Deepfakes pose a new threat to the financial sector as AI technology becomes more advanced,** enabling bad actors to gain entry to banking systems with realistic audio and images, per the Wall Street Journal.

**How we got here:** Many banks have enhanced the customer experiences on their apps and websites by streamlining digital account access. That's included enabling voice and facial recognition for a simpler, quicker login.

- Meanwhile, AI has developed to the point where it enables bad actors to mimic users' voices or images to gain entry into accounts.
- **Such incidents increased by 700% between 2022 and 2023,** according to the Wall Street Journal. When a Wall Street Journal reporter experimented with an AI-generated version of herself, she was able to trick **Chase's** system.

**Preventing big losses:** Beyond alienating their customers who become fraud victims, banks that don't prioritize safeguards also risk substantial financial losses.

- American Banker recommends that banks update their know-your-customer processes with deepfake detection mechanisms and advanced technology. They must also raise customer and employee awareness of this risk.
- Crowe recommends banks collaborate with financial industry trade associations, regulators, and law enforcement to develop standards, regulations, and strategies that help to combat this trend.

**Key takeaways:** Though bigger banks with larger cybersecurity budgets may be able to dedicate more resources toward deepfake incident prevention, FIs of all sizes remain at risk.

- Until FIs can ensure robust protections are in place, they should minimize potential pathways for these actors and require more complex verification for customer logins.