FIDUCIENT
Advisors
Helping Clients Prosper

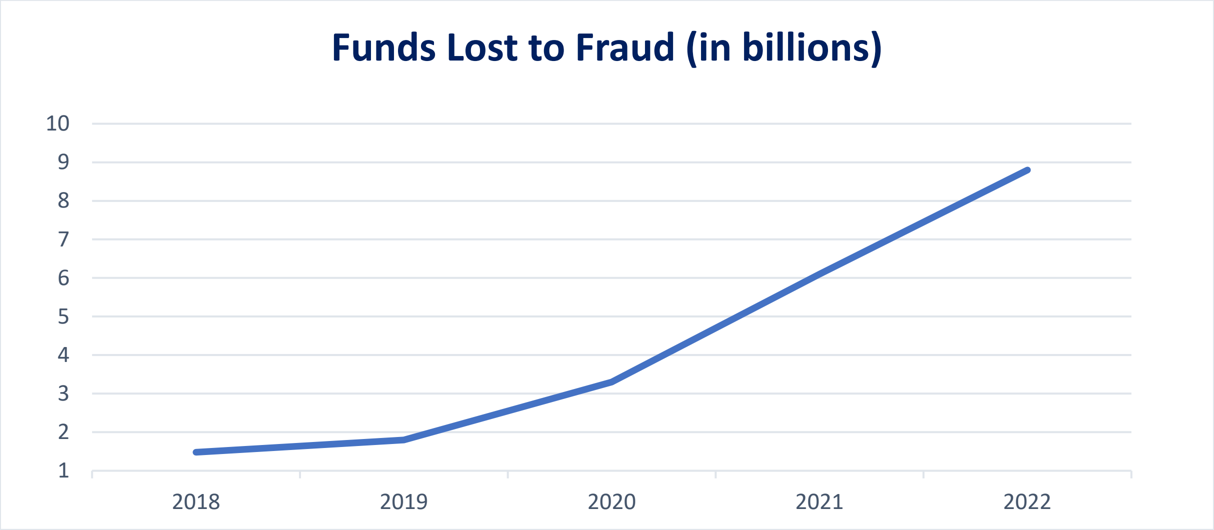
Guarding Your Digital Identity: Defending Against AI-Driven Fraud

by Miranda Brozik, Consulting Analyst

March 2024

In January of 2024, a disturbing incident shook the financial world as a Hong Kong bank employee fell victim to deepfake technology, resulting in a fraudulent payout of $25 million.[1] This sophisticated deception, where AI-generated replicas of colleagues participated in a video conference, underscores the growing threat posed by AI-driven fraud. Another harrowing example involved Paddric Fitzgerald, who received a distressing call purportedly from his kidnapped daughter, a cruel manipulation facilitated by AI-generated audio.[2] These distressing instances underscore the alarming capabilities of deepfake technology and its potential to exploit even the most cautious individuals.

Beyond deepfake technology, AI has the capability to swiftly scour the Internet for personal data, facilitating a form of fraud known as "synthetic fraud." Synthetic fraud entails the creation of a new identity by blending genuine and falsified information. For instance, a perpetrator might utilize a stolen social security number alongside a fictitious name to initiate account creation and conduct transactions. This type of fraud poses significant challenges for monitoring and detections, as fraudsters often invest years in building a solid credit



Source: Federal Trade Commission. As of February 2018 – February 2023.

[1] *https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html, February 2, 2024*
[2] *AI heralds the next generation of financial scams (ft.com), January 18, 2024*

This report is intended for the exclusive use of clients or prospective clients (the "recipient") of Fiducient Advisors and the information contained herein is confidential and the dissemination or distribution to any other person without the prior approval of Fiducient Advisors is strictly prohibited. Information has been obtained from sources believed to be reliable, though not independently verified. Any forecasts are hypothetical and represent future expectations and not actual return volatilities and correlations will differ from forecasts. This report does not represent a specific investment recommendation. The opinions and analysis expressed herein are based on Fiducient Advisor research and professional experience and are expressed as of the date of this report. Please consult with your advisor, attorney and accountant, as appropriate, regarding specific advice. Past performance does not indicate future performance and there is risk of loss.

history under a fabricated identity before executing final fraudulent activities and subsequently abandoning the identity. Synthetic fraud stands as the fastest-growing category of financial crime in the United States, signifying the urgent need for robust countermeasures. In fact, the rise of advancing technology has contributed to an increase in fraud of over 30% from 2022 to 2021.[3]

As fraudulent activities evolve in sophistication, maintaining vigilance and implementing proactive defense strategies are imperative for consumers. Staying abreast of recent AI trends is paramount, requiring dedication to exploring news articles, podcasts and participating in relevant workshops or webinars. These avenues provide valuable insights into AI's evolving role in fraud and strategies to mitigate risks. Online courses available through platforms like Coursera, Udemy and edX offer opportunities to deepen understanding, covering introductory to advanced levels taught by industry experts. Understanding that scammers often exploit emotions emphasizes the significance of staying aware of recent trends to recognize potential warning signs before emotions compromise judgement.

Enforcing robust security measures is crucial in safeguarding personal information effectively. This entails employing strong, unique passwords with a combination of numbers, symbols and letters for each website, and maintaining updated security software with automatic updates enabled. Regularly monitoring communications from entities relying on sensitive data, such as the IRS, banks and credit card providers enables early detection and prevention of fraud. Neglecting the communications from these institutions increases vulnerability, particularly among susceptible demographics like children, the elderly and the homeless. Investing in identity protection services offering comprehensive coverage against all forms of fraud serves as an additional layer of defense.

In conclusion, as artificial intelligence-driven fraud becomes increasingly prevalent and sophisticated, it is imperative for individuals to remain vigilant and proactive in their defense strategies. By leveraging advanced technologies, implementing robust security measures, and fostering a culture of awareness and education, we can better protect ourselves against the evolving landscape of fraudulent activities. With a concerted effort and a commitment to staying informed and adaptive, we can mitigate the risks posed to AI-driven fraud and safeguard our financial well-being and digital assets. For more information, please contact any of the professionals at Fiducient Advisors.

[3] *New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022*

About the Author

Miranda Brozik
Consulting Analyst

As a Consulting Analyst, Miranda is responsible for the analysis of Financial Institution client investment portfolios. Prior to joining Fiducient Advisors in 2022, Miranda worked in AML compliance for over 7 years. Miranda earned a BS in Investment Analysis from the University of South Florida. Her personal interests include running, reading, spending time with her niece and two nephews and volunteering with the Midtown Educational Foundation, serving on their young professional board.