



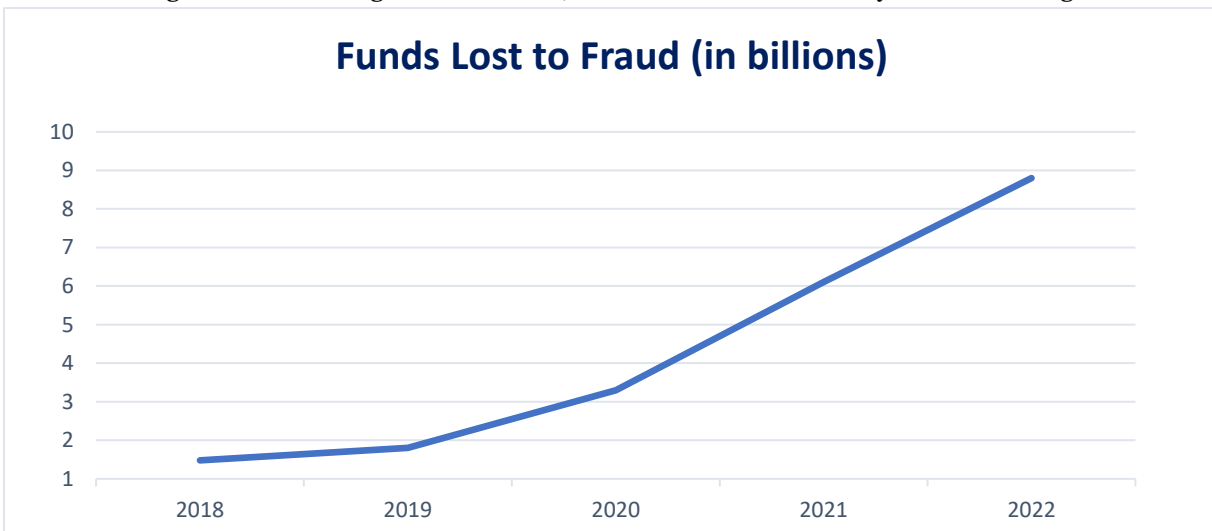
Let our independence ignite yours.™

Guarding Your Digital Identity: Defending Against AI-Driven Fraud

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 \(ft.com\)](https://www.ft.com/content/2024/01/18/ai-heralds-the-next-generation-of-financial-scams), January 18, 2024

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.

Disclosures

This document is intended for the exclusive use of clients or prospective clients of PCS Advisors. Any additional dissemination or distribution is strictly prohibited. Information provided in this document is for informational and/or educational purposes only and is not, in any way, to be considered investment advice nor a recommendation of any investment product or service. Advice may only be provided after entering into

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

an engagement agreement and providing PCS Advisors with all requested background and account information.

In partnership with Fiducient Advisors, the included information has been obtained from a variety of sources believed to be reliable though not independently verified. Any forecasts represent future expectations and actual returns, volatilities and correlations will differ from forecasts. Past performance does not indicate future performance and there is a possibility of a loss.

Please visit www.pcsbd.net/disclosures for other important disclosures. Private Client Services is an SEC Registered Investment Advisor doing business as PCS Advisors. For information about Fiducient Advisors please visit www.fiducientadvisors.com.