Using biometrics to fight back against rising synthetic identity fraud

Traditional security systems seem to be no match for sophisticated identity fraudsters. What can banks do to help stay a few steps ahead?

Deloitte Center for Financial Services

Deloitte.
Insights

Deloitte Risk & Financial Advisory

Deloitte Risk & Financial Advisory helps organizations navigate a variety of risks to lead in the marketplace and disrupt through innovation. The insights of our professionals, combined with our specialized products and services, help clients learn how to embrace complexity and leverage their position of strength to accelerate performance. ***Learn more***.

Table of contents

Synthetic identity fraud—when cybercriminals create new identities with stolen or fabricated data—is the fastest growing financial crime in the United States,[1] and it shows no sign of abating. Not only can bad actors purchase personally identifiable information on the dark web for a pittance,[2] but advancements in Generative AI are making it easier to produce images and videos in someone else's likeness—whether they may be real or imaginary.

Deloitte Center for Financial Services expects synthetic identity fraud to generate at least US$23 billion in losses by 2030,[3] prompting many banks and fintechs to develop more advanced biometric security systems to weed out would-be perpetrators. These projections incorporate historical data on the rate of synthetic fraud and expectations of growth in noncash payments in the United States until 2030.[4] We used the Federal Reserve Payments Survey to find this expected payment volume—excluding prepaid debit cards—and assumed that synthetic identity fraud would grow incrementally each year.

Synthetic identity fraud is both increasing with the rise of digital interactions and becoming more complex as Generative AI and other technologies advance. Many fraudsters concoct entire personas using a mix of real and fabricated information, which are often pinned to social security numbers taken from children or the recently deceased. These bad actors may spend months or years nurturing their synthetic identities, and more than half have a credit score over 650,[5] just shy of what agencies consider "good."[6] The average payoff is estimated to be between US$81,000 and US$98,000,[7] but a single attack can sometimes result in the theft of several millions.[8] Synthetic fraudsters may also try to disguise themselves as new customers so they can add themselves to existing bank accounts, or look for lenders who will grant loans to "credit invisible" consumers with no reportable financial history.[9]

What makes synthetic identity fraud notoriously difficult to detect? For a start, fraudsters often create an extensive history in the public domain using their fabricated credentials. They can also correctly enter information to common identity verification questions about their manufactured lives. In fact, 85% of synthetic identities in the emerging consumer sector elude third-party risk models, according to LexisNexis Risk Solutions.[10] These external tools will be increasingly useful for detecting anomalous behavior and reducing false positive rates, especially if they utilize deep learning to analyze multiple characteristics and data points of users' identities at once. Banks and financial institutions should follow rigorous model risk management procedures to help ensure they are properly monitoring algorithms for performance, transparency, and interpretability.

Stronger biometrics can help to create a wider safety net

Both physical and behavioral biometrics systems can add overlapping lines of defense; they can work together to catch opportunistic hoaxers who would have fallen through the cracks of traditional security checks. Unlike passwords or PINs, physical biometric technology can analyze traits that are unique to each consumer's makeup, such as their palm vein patterns, retina details, vocal pitch, and ear canal shapes. These biometric security tools can improve outcomes for ID verification and authentication, but many emerging solutions are susceptible to low-cost, creative workarounds. Researchers, for example, recently hacked facial identification technology by placing glasses with tape where eyes should be over smartphones owners' faces while they slept.[11] Smartphone users have also found a myriad of ways to dupe fingerprint sensors, including with gummy bears,[12] wood glue,[13] and cheap printed circuit boards.[14] These "deepfakes" have passed through some banks' know your customer (KYC) protocols.[15]

To help counteract these fraudulent actions, new and powerful biometric tools can provide additional layers of defense by evaluating whether users are human, testing the veracity of visual artifacts and manipulated recordings, and identifying anomalies that may be atypical of online consumer behavior. These loopholes may create more demand for biometrics capabilities that can assess "liveness."

Financial institutions should expend more effort refining "liveness detection" checks that distinguish human consumers from synthetic identities who use stolen or AI-generated content to act as the face of their alter egos. These tests may use a range of techniques to verify that a user is responding in real time, for example, by asking them to tilt their head to the side, smile, or blink. Security systems for physical biometrics can compete with the growing sophistication of spoofers by adding elements like skin texture, facial imperfections, perspiration, and blood flow.[16] Banks and card issuers can then evaluate whether the results match up with government-issued ID documents, as well as third-party consortium data and any national ID verification services available to them. They can also check for other indicators of synthetic identity fraud, such as a lack of connections to family members and associates.[17]

Banks and card issuers are also planning to significantly expand capabilities in emerging behavioral biometrics tools. These systems can provide continuous authentication by tracking dynamic information about users and learning more about them over time. Moreover, this information can usually be gathered with no additional input from consumers, and it is nearly impossible to replicate. For example, behavioral biometrics technologies aim to analyze a consumer's touchscreen behavior, mobile app navigation, and typing habits. As a result, even if cyber criminals had the correct password for the user they're trying to impersonate, the technology could flag that they're entering a password slower than usual or applying less pressure to the device's screen.

Behavioral biometrics is expected to be particularly effective in spotting synthetic identities, since fraudsters usually type information quickly across multiple forms, copy and paste it from other sources, or use uncommon keyboard shortcuts.[18] The test results can then be supplemented with nonbiometric factors, such as location histories and spending habits, to trigger instant alerts of unusual transactions that require further review. Moreover, banks can also work more closely with startups and established technology firms to develop multimodal biometric security that evaluates several indicators at once, such as fingerprints, natural speech patterns, and word choice. These enhanced systems may also perform better in a variety of settings and lighting environments and work more effectively with underrepresented consumer groups.[19]

Banks and fintechs should take a proactive approach to managing and testing their proprietary and third-party tools, including validation of controls, by feeding them with "synthetic" or artificial biometric data. Synthetic data can be immensely valuable when it is too costly, time-consuming, or sensitive to collect real data that make biometrics algorithms produce more accurate predictions.[20] For instance, many current AI systems used for facial recognition have been typically trained on white subjects.[21] By including digitally generated datasets that include more diverse demographics, the tools can become better at identifying diverse faces. Banks and financial institutions should also take additional steps to check the maturity of the controls of their banking partners.

One of the biggest challenges facing financial institutions in the longer term is extending biometric security to new and emerging consumer technologies and having them work together to monitor for anomalous activity contemporaneously. For example, financial institutions may need to develop interactive dashboards that may link behavioral biometric systems to new tools for flagging one-time password fraud, SIM swap fraud, and mobile wallet fraud in real time. In addition, these organizations should consider determining how to safeguard biometric data shared between devices connected by a network, including the Internet of Things (IoT). In the longer term, it may also be imperative for businesses to contemplate how the cryptography-breaking power of quantum computers[22] could undermine existing processes for biometric authentication.

Biometrics are important to a zero-trust security model

Physical and behavioral biometrics are becoming a more critical component of the zero-trust security model, which assumes all network traffic is malicious. Financial institutions should continually monitor users and devices instead of trusting that the network's security perimeter will be sufficient to prevent breaches. Biometrics can buttress the "never trust, always verify" ethos by adding heightened controls that require hard-to-copy information such as fingerprints at every access point in the network.

Biometric systems may also become increasingly important as digital currencies such as central bank digital currencies (CBDCs) enter the mainstream, and consumers conduct more transactions using digital wallets. The European Union, for example, plans to examine how biometrics can be used to verify and authenticate users of the EU Digital Identity Wallet,[23] where the digital euro will likely be stored. The expansion of these verification systems can offer additional safeguards beyond the banking sector by confirming a user's identity when sharing medical data, taking online exams, or making age-restricted purchases.[24]

Biometrics can also create seamless customer experiences

Banks and card issuers have another incentive to continue investing in biometrics: Many customers really seem to like it.

Physical biometrics can improve customer experience and reduce abandonment rates in account opening and onboarding processes or other digital transactions due to burdensome security measures. One-quarter of UK adults would exit the account opening process if the identity checks were too time-consuming or complex.[25]

Some brands are tapping biometrics as an innovative payment method. Panera Bread and Whole Foods Markets, for example, recently unveiled palm payments, which allows users to make purchases by waving their hand over a sensor.[26] In just a few years, three billion global consumers are expected to make US$5.1 trillion of purchases using biometric payments.[27] Merchants have also expressed interest in using biometrics to offer personalized services or loyalty rewards to consumers at checkout.

Finally, biometrics can also help facilitate financial inclusion by allowing those who lack formal documents used to establish identity, and who have thus been unable to access traditional financial services, to execute safe and secure digital transactions. It can also expand branchless banking services to mobile consumers and protect the assets of women or other vulnerable individuals by offering them sole access to bank accounts.[28] And since consumers could no longer be required to recall complex sequences or credentials, it can improve accessibility for groups with cognitive and learning disabilities.

In the end, biometrics should be a win-win for banks. Not only can biometrics play a critical role in detecting and mitigating fraud, synthetic or otherwise, but it may help expand financial inclusion and provide more secure and seamless customer experiences.

Endnotes

[1] FedPayments Improvement, “Synthetic identity fraud,” accessed June 8, 2023.

[2] Polymer Solutions, Inc., “What is the cost of PII on the dark web in 2022?,” accessed June 23, 2023.

[3] Deloitte Center for Financial Services analysis of data from Auriemma Group and the 2022 Federal Reserve Payments Study.

[4] Auriemma Roundtables, “Industry reaches key milestone in fight against synthetic identity fraud, but many challenges remain,” news release, July 27, 2018.

[5] LexisNexis Risk Solutions, *Uncovering synthetic identity fraud*, 2021, p. 2.

[6] Experian, “650 credit score: Is it good or bad?,” accessed June 12, 2023.

[7] FiVerity, *2021 Synthetic fraud report*, October 2021, p. 10.

[8] US Attorney's Office, Southern District of Florida, “Defendant pleads guilty to stealing $24 million in Covid-19 relief money through fraud scheme that used synthetic identities,” press release, June 29, 2021.

[9] LexisNexis Risk Solutions, *Uncovering synthetic identity fraud*, p. 2.

[10] Ibid.

[11] Yu Chen, Bin Ma, and HC Ma, “Biometric authentication under threat: liveness detection hacking,” presented at Black Hat USA 2019, August 7, 2019.

[12] Cuyler Yu, “Could a gummy bear access your phone?,” Medium, May 21, 2021.

[13] Nathaniel Mott, “Hacking fingerprints is actually pretty easy—and cheap,” *PCMag*, November 22, 2021.

[14] Arol Wright, “This $15 hacking device could be your fingerprint scanner's worst nightmare,” Android Police, May 26, 2023.

[15] James Vincent, “Liveness tests used by banks to verify ID are ‘extremely vulnerable’ to deepfake attacks,” *The Verge*, May 18, 2022.

[16] Aratek, “Liveness detection: Your guide to protecting biometric systems,” accessed June 8, 2023.

[17] LexisNexis Risk Solutions, *Uncovering synthetic identity fraud*, p. 4.

[18] Jim Murphy, “How insurance carriers can tackle fraud with behavioral biometrics,” Celebrus, accessed June 8, 2023.

[19] Aware, “Biometrics simplified,” accessed June 8, 2023.

[20] Mohammad Nabati et al., “Using synthetic data to enhance the accuracy of fingerprint-based localization: a deep learning approach,” *IEEE Sensors Letters* 4, no. 4 (2020): p. 1–4.

[21] Jan Lunter, “Synthetic data: A real route to eliminating bias in biometrics,” *Biometric Technology* Today, no. 1 (January 2023).

[22] James Thorpe, “Why will biometric security be vital in a post-quantum future?,” *International Security Journal* (December 2022).

[23] Stanislas Tarnowski, “[Interview] Gregory Kuhlmey, IDEMIA: Biometrics in digital identity wallet,” inCyber, October 11, 2022.

[24] Vicki Hyman, “Phone, keys…face? Why biometrics may make your wallet obsolete,” Mastercard, accessed June 8, 2023.

[25] FICO, *Consumer survey 2022: Fraud, identity, and digital banking in the UK*, 2022, p. 2.

[26] Rimma Kats, “Starbucks is the latest retailer to trial palm payments,” *PaymentsJournal*, May 2, 2023.

[27] JPMorgan Chase & Co., “J.P. Morgan to pilot biometrics-based payments for merchants,” press release, March 23, 2023.

[28] Visa, “Assessing the role of biometrics in advancing financial inclusion,” 2019, p. 5–6.

About the authors

Satish Lalchand

slalchand@deloitte.com

Satish Lalchand is a principal in the analytics practice of Deloitte Transactions and Business Analytics LLP, specializing in anomaly detection and data analytics, business rules development, and modeling. Lalchand has in-depth knowledge of fraud rules creation for prevention, detection, and investigation with a broad range of experience in managing and leading engagements in these areas. A certified fraud examiner (CFE), he has presented on "Using data analytics" at ACFE and IIA events.

Val Srinivas, PhD

vsrinivas@deloitte.com

Val Srinivas is the banking and capital markets research leader at the Deloitte Center for Financial Services. He leads the development of our thought leadership initiatives in the industry, coordinating our various research efforts and helping to differentiate Deloitte in the marketplace. He has more than 20 years of experience in research and marketing strategy.

Jill Gregorie

jgregorie@deloitte.com

Jill Gregorie is a lead market insights analyst with the Deloitte Center for Financial Services. She is focused on research and analysis in support of a wide variety of strategic and actionable insights for clients in the banking and capital markets sector.

Acknowledgments

The authors would like to thank **Brendan Maggiore** of Deloitte Transactions and Business Analytics LLP for his contributions to this article.

About the Center for Center for Financial Services

The Deloitte Center for Financial Services, which supports the organization's US Financial Services practice, provides insight and research to assist senior-level decision-makers within banks, capital markets firms, investment managers, insurance carriers, and real estate organizations. The center is staffed by a group of professionals with a wide array of in-depth industry experiences as well as cutting-edge research and analytical skills. Through our research, roundtables, and other forms of engagement, we seek to be a trusted source for relevant, timely, and reliable insights. Read recent publications and learn more about the center on Deloitte.com. For weekly actionable insights on key issues for the financial services industry, check out the Deloitte Center for Financial Services' QuickLook article series.

Connect

To learn more about the vision of the DCFS, its solutions, thought leadership, and events, please visit **www.deloitte.com/us/cfs**.

Subscribe

To receive email communications, please register at **www.deloitte.com/us/cfs**.

Engage

Follow us on Twitter at: @DeloitteFinSvcs

Contact us

Industry leadership

Monica O'Reilly
US Financial Services Industry leader | Principal | Deloitte and Touche LLP
+1 415 783 5780 | monoreilly@deloitte.com

Monica O'Reilly leads the US Financial Services Industry group focused on the banking, capital markets, insurance, investment management, and real estate sectors.

Center for Financial Services

Jim Eckenrode
Managing director | Deloitte Center for Financial Services
+1 617 585 4877 | jeckenrode@deloitte.com

Jim Eckenrode is the managing director of the Deloitte Center for Financial Services and is responsible for developing and executing Deloitte's financial services research agenda, while providing insights to leading financial institutions on business and technology strategy.

Deloitte.
Insights

Sign up for Deloitte Insights updates at **www.deloitte.com/insights**

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Karen Edelman, Hannah Bachman, Rupesh Bhat, and Emma Downey
Creative: Natalie Pfaff, Alexis Werbeck, Meena Sonar, Govindh Raj, and Pooja Lnu
Deployment: Atira Anderson
Cover artwork: Natalie Pfaff

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.