

CyberIdaho Financial Innovation Lab

Emerging Technology Advisory Committee Report

Cryptographic Decentralized Identity Solutions are Vital for Protecting Sensitive Information, Reducing Identity Fraud, & Safeguarding Privacy

Executive Summary

The rapid digitization of financial products and services is driving the aggregation of sensitive personally identifying information (PII) into large centralized databases that cybercriminals increasingly target, fueling a surge in identity theft and underscoring the need for cryptographic decentralized identity solutions to better protect American businesses, consumers, and financial stakeholders. Cryptographic decentralized identity solutions use advanced cryptographic techniques and mathematical algorithms/proofs (e.g., zero-knowledge proofs) to verify identity attributes without revealing underlying personal data, while decentralized infrastructure such as distributed ledger technologies (e.g., blockchains) provide secure credential verification without relying on centralized databases to enhance privacy, security, and data minimization.

The development and implementation of cryptographic decentralized identity solutions in the financial services space is critical considering the financial sector is currently the most breached industry and identity fraud and scams cost Americans over \$47 billion this past year alone. However, despite the continued digitization of financial services the sector remains heavily reliant on legacy “Know Your Customer” (KYC) identity verification systems that store vast amounts of sensitive PII in centralized databases. These systems create attractive “data honeypots” for global cybercriminals who are seeking to exploit stolen credentials for identity theft and financial fraud. Without modernization, the financial industry will continue to face rising breach incidents, escalating compliance costs, mounting consumer privacy risks, and significant identity theft losses.

As the financial system becomes increasingly digital, policymakers must prioritize the advancement of cryptographic decentralized identity solutions to maintain trust, enhance security, and combat rising cybercrime. Achieving this objective will require coordinated policy action, including designating cryptographic decentralized identity as a national priority and directing relevant federal agencies to develop clear technical standards and regulatory frameworks to foster responsible innovation. Policymakers should further accelerate adoption by supporting pilot programs and establishing safe harbor protections that encourage financial institutions and technology providers to test, develop, and deploy cryptographic decentralized identity solutions at scale.

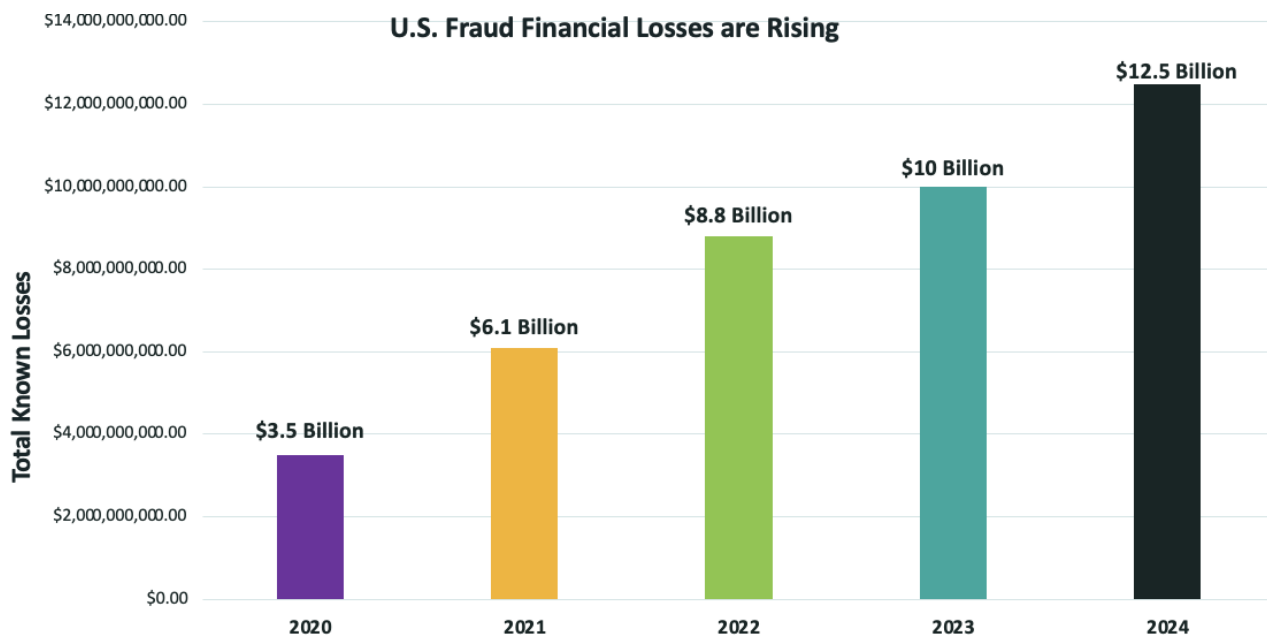
1 2

Data Breaches & Identity Fraud Losses are Rising in the United States

Increases in digital economic activity and data storage are acting as catalysts for proliferating data breaches and identity fraud financial losses. Research highlights that the United States suffered 3,322 known data compromises in 2025, which is the highest number ever recorded and part of a 79% increase in breaches over the past five years.³ These incidents exposed the personal data of 278.8 million individuals in 2025 alone highlighting the massive scale at which personal information is being compromised.⁴ These trends are closely tied to the widespread storage of sensitive PII in centralized databases used for identity verification and regulatory compliance. When these systems are compromised, attackers can obtain millions of identity records at once and use them to commit downstream fraud and identity theft.

The financial consequences of identity-based cybercrime are also accelerating. Federal Trade Commission data reveals that Americans lost a record \$12.5 billion to fraud in 2024, with over 1.1 million identity theft cases reported, highlighting identity fraud as a driving force behind rising U.S. fraud losses (see the chart below that

shows a 257% increase in American fraud losses over the past five years).⁵ These statistics underscore how stolen personal information continues to fuel the financial fraud and cybercrime that is harming the American public and businesses.



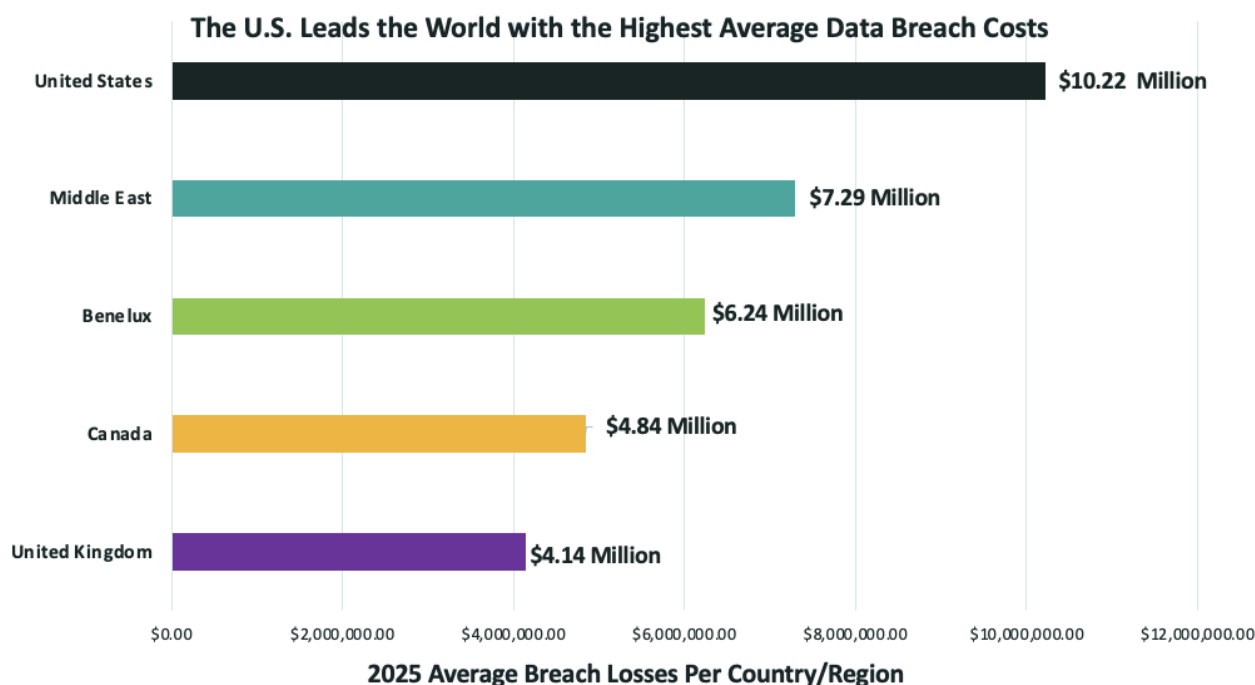
The growing frequency and scale of data breaches and identity fraud/theft showcases the need for more secure and privacy-preserving identity verification systems. Cryptographic decentralized identity solutions offer a promising approach because it allows individuals to verify identity attributes without requiring organizations to store large volumes of sensitive personal data, thereby reducing breach risks and limiting opportunities for identity-based cybercrime.

[The Digitization of Financial Services, Outdated Identity Systems, & Centralized Data Honeypots Are Making Cryptographic Decentralized Identity Solutions Critical](#)

The financial industry's digital transformation combined with growing consumer reliance on digital financial services/products are expanding the financial sector's cyber threat surface area and creating large PII data honeypots, making the industry an increasingly attractive target for cybercriminals that reinforces the need for cryptographic decentralized identity solutions. Digital financial services are almost ubiquitous at financial entities throughout the United States with nearly 85% of American adults using mobile banking services, while approximately 90% use some form of financial technology to conduct economic activity.^{6 7} Today, a majority of Americans access financial services through digital channels and platforms making them the dominant interfaces for managing accounts and conducting transactions. COVID-19 acted as a catalyst to this trend as 72% of financial institutions accelerated digital transformation during this period and more people began using digital financial technology, internet connectivity, and mobile services for business, shopping, entertainment, and personal purposes.^{8 9} While this digital transformation has improved efficiency and accessibility, it has also increased digital storage requirements and the financial sector's cyber-attack threat surface area.

Despite this shift toward digital financial services, most institutions still rely on outdated legacy identity verification systems built around traditional "Know Your Customer" (KYC) compliance processes that are high value targets for cybercriminals seeking PII data for identity fraud schemes. As financial activity increasingly moves online, institutions must verify customer identities remotely, which requires collecting and storing large amounts of PII such as Social Security numbers, dates of birth, government identification records (e.g., drivers licenses and passports), and financial account data. The collection of this data into centralized databases is a central reason why the financial sector became the most breached industry in the United States with 739 known breaches this past year.¹⁰

The financial industries reliance on centralized identity databases that function as large data honeypots is fueling identity fraud cybercrimes and rising data breach costs, underscoring the urgent need for a new decentralized approach to protecting sensitive information. On average, financial industry breaches expose approximately 32,000 identity records that are then either sold or reused by cybercriminals to commit identity fraud.¹¹ Furthermore, the average cost of a data breach in the United States is currently nearly \$10 million (see chart below), which results in increased costs for both American financial businesses and consumers.¹² These trends highlight the structural weaknesses of legacy identity systems and showcases the need for more secure identity verification models. Cryptographic decentralized identity solutions can address this challenge by enabling individuals to verify identity attributes through advanced cryptography without requiring institutions to store large volumes of sensitive personal data in centralized databases.



Large Scale Data Breaches, Identity Theft Losses, & Compliance Costs Will Continue to Increase if Cryptographic Decentralized Identity Solutions & Frameworks are Not Adopted

If the financial sector does not modernize its approach to digital identity verification and adopt a more decentralized solution, large-scale data breaches, identity theft, and cybercrime losses will likely continue to grow in both frequency and scale. Financial institutions store vast quantities of sensitive PII to comply with identity verification and regulatory KYC requirements that will ensure they remain high-value targets for cybercriminals who rely on this information to conduct identity fraud. As a result, the industry faces persistent security threats, with research indicating that approximately half of financial institutions experienced a data breach within the past two years, while the financial services industry accounted for nearly a quarter of all global cyber breaches, reflecting the significant value of financial and identity data stored by financial institutions and fintech platforms.^{13 14}

Absent a shift towards more secure identity verification frameworks that prioritize data minimization and decentralization, compliance risks and costs will almost certainly grow exponentially. Traditional compliance systems will continue to require institutions to collect and store large volumes of sensitive personal data in centralized databases to meet growing anti-money laundering, KYC, and fraud prevention program requirements, which will expand their cyber attack threat surface area and increase their data management, identity verification, and cybersecurity costs. This is a major reason why financial institutions now spend more than \$200 billion annually on both financial crime compliance and cybersecurity (over \$400 billion total).^{15 16}

Cryptographic decentralized identity solutions offer a promising opportunity because they eliminate centralized honeypots, enable data minimization, simplify audit and reporting processes, and use automation to decrease manual labor costs all of which significantly reduces compliance costs, lowers data breach/identity fraud risks, and improves privacy protections. By using verifiable credentials (e.g., zero-knowledge proofs), individuals can prove identity attributes without revealing their underlying personal data, enabling strong data minimization and selective disclosure to considerably improve privacy protections.

Decentralized identity systems also mitigate the risks associated with centralized data honeypots by enabling cryptographic identity verification rather than manual document checks, allowing organizations to automate verification processes, reduce identity fraud risks, and lower operational and compliance costs. Studies show that organizations adopting decentralized identity frameworks can reduce identity-related fraud incidents by as much as 40–60%, while concurrently drastically decreasing identity management infrastructure costs via automation and reusable credentials.¹⁷ The various benefits these solutions provide makes incentivizing their development and adoption necessary to better protecting the financial sector and Americans.

Policymakers Should Declare Decentralized Digital Identity a National Priority, Establish Standards/Frameworks, Authorize Pilots, & Provide Incentives & Safe Harbor Protections

As financial services continue to digitize leading to rising data breaches and identity fraud losses for American businesses and consumers it is vital for policymakers to prioritize the creation of policies that will ensure the development, implementation, and adoption of cryptographic decentralized identity solutions that can improve privacy, mitigate cybercrime/fraud, lower compliance costs and enable a stronger regulatory regime. To create a more efficient and effective identity verification system in the financial industry policymakers should take the following steps:

Declare Cryptographic Decentralized Identity Development a National Priority – Congress, the White House, and federal financial regulators should formally designate cryptographic decentralized digital identity solutions as a national cybersecurity and financial system priority. Congress can elevate decentralized identity as a priority by directing federal agencies to study and support the development and adoption of verifiable credentials, decentralized identifiers, and privacy-preserving cryptographic identity verification technologies. Legislative action should also authorize research funding, commission studies, and require financial regulators to evaluate how cryptographic decentralized identity solutions such as [Zyphe](#) can strengthen fraud prevention and modernize outdated KYC processes.

The White House can reinforce this priority by incorporating decentralized identity technologies into broader national cybersecurity and digital infrastructure strategies, including initiatives aimed at strengthening digital trust and reducing cybercrime. Through executive orders and interagency coordination, the Administration can direct federal agencies to prioritize privacy-preserving identity systems that reduce reliance on centralized identity databases.

The Treasury Department should play a key role in coordinating domestic and international financial regulators via research initiatives to evaluate how decentralized identity credentials could enhance financial crime prevention while improving data security. Treasury recently highlighted the importance of digital identity solutions in their report to Congress on countering digital asset illicit finance, but policymakers should seek to incorporate decentralized solutions across the entire financial ecosystem.¹⁸

Establish Clear Standards, Frameworks, & Interoperability Requirements– Policymakers should direct federal agencies such as the National Institute of Standards and Technology (NIST), Treasury Department, Federal Financial Institutions Examinations Council (FFIEC), and others to establish clear technical standards, governance frameworks, and financial sector interoperability requirements for cryptographic decentralized identity systems. Without clear standards, frameworks, and requirements

financial stakeholders will lack the legal and regulatory clarity they require to adopt these solutions. Technical standards are critical for ensuring that digital identity credentials can be trusted across institutions and jurisdictions, while interoperability requirements are essential for ensuring acceptance across different platforms and eliminating fragmentation issues.

Furthermore, it is important to build strong governance frameworks that build trust, transparency, and accountability and provide both government and industry stakeholders with the legal certainty and confidence they require for cryptographic identity solutions to be adopted. Policymakers should also make sure that they are engaging with key industry stakeholders and aligning requirements with other digital identity development efforts such as NIST's Digital Identity Guidelines.¹⁹

Authorize & Create Cryptographic Decentralized Digital Identity Pilots & Sandboxes – In order to evaluate the effectiveness of cryptographic decentralized identity credentials for KYC compliance, fraud prevention, and secure digital authentication federal policymakers and financial regulators should create sandboxes and pilots where new solutions can be tested and approved. It is vital that any pilot or sandbox provide a clear pathway for new solutions to graduate so they can be widely adopted. These pilot programs and sandboxes would allow regulators and industry stakeholders to assess security benefits, interoperability challenges, and compliance impacts before broader implementation.

Provide Adoption Incentives & Safe Harbor Protections– With financial institutions facing burdensome compliance responsibilities that are making them prime targets for cybercriminals, policymakers should seek to provide targeted incentives that encourage financial institutions to adopt privacy-preserving cryptographic decentralized identity solutions. Policymakers could provide incentives by allowing institutions that implement approved cryptographic decentralized identity systems to benefit from streamlined identity verification procedures or reduced duplicative compliance requirements when identity attributes are verified through trusted cryptographic credentials. These incentives would encourage institutions to modernize identity infrastructure while maintaining strong regulatory safeguards against financial crime.

Policymakers should also create incentives that reward data minimization and improved cybersecurity practices. Regulatory frameworks should recognize cryptographic decentralized identity systems as compliant methods of verifying identity while reducing the need for institutions to collect and store large volumes of PII.

Finally, it is imperative that policymakers establish safe harbor protections for financial institutions that implement cryptographic decentralized identity frameworks consistent with federal standards. Such protections could limit liability or reduce regulatory penalties for cyber incidents involving identity data, provided the institution adopted approved privacy-preserving identity systems. By aligning incentives with modern identity technologies, policymakers can encourage financial institutions to decrease centralized data storage, strengthen cybersecurity protections, and lower long-term compliance costs.

The financial sector is becoming more digital, which means data breaches and identity fraud will continue to grow exponentially unless the financial industry moves away from its reliance on centralized databases and outdated legacy compliance structures and starts adopting innovative cryptographic decentralized identity solutions. By embracing the policy solutions above policymakers will provide the financial industry with the support and clarity it requires to transition to cryptographic decentralized identity solutions that have the ability to drastically increase privacy, reduce data breaches, mitigate cybercrime and identity fraud, cut compliance costs, and improve the effectiveness of financial compliance programs for the benefit of the American public and financial businesses.

Endnotes

-
- ¹ <https://bankingjournal.aba.com/2026/01/report-data-breaches-becoming-more-focused> (refers to the financial services industry being the most breached sector in the callout box).
- ² <https://www.aarp.org/money/scams-fraud/javelin-identity-theft-report-2024> (refers to the \$47 billion in identity fraud and scam losses referenced in the callout box).
- ³ <https://www.idtheftcenter.org/post/2025-annual-data-breach-report-record-number-compromises>
- ⁴ <https://www.idtheftcenter.org/publication/2025-data-breach-report>
- ⁵ <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>
- ⁶ <https://www.marketdataforecast.com/market-reports/north-america-digital-banking-market>
- ⁷ <https://plaid.com/the-fintech-effect-2021-mass-adoption/>
- ⁸ <https://pmc.ncbi.nlm.nih.gov/articles/PMC9759262/#:~:text=In%20this%20paper%2C%20we%20provi%20de,occurred%20in%20the%20pandemic's%20absence>
- ⁹ <https://gitnux.org/digital-transformation-in-the-banking-industry-statistics>
- ¹⁰ <https://www.idtheftcenter.org/post/2025-annual-data-breach-report-record-number-compromises/#:~:text=In%202025%2C%20the%20Financial%20Services,still%20fall%20victim%20to%20criminals>
- ¹¹ <https://zipdo.co/cybersecurity-breach-statistics>
- ¹² <https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91>
- ¹³ <https://www.sailpoint.com/identity-library/identity-security-financial-services>
- ¹⁴ <https://www.kroll.com/en/publications/cyber/data-breach-outlook-2025>
- ¹⁵ <https://risk.lexisnexis.com/about-us/press-room/press-release/20230926-global-financial-crime-compliance-costs>
- ¹⁶ [https://www.computerweekly.com/news/366628165/Global-cyber-spend-will-top-200bn-this-year-says-Gartner#:~:text=Driven%20by%20an%20ever%20escalating%20number%20of%20high%20profile,\\$200bn%20\(£150bn\)%20during%202025%2C%20according%20to%20Gartner.](https://www.computerweekly.com/news/366628165/Global-cyber-spend-will-top-200bn-this-year-says-Gartner#:~:text=Driven%20by%20an%20ever%20escalating%20number%20of%20high%20profile,$200bn%20(£150bn)%20during%202025%2C%20according%20to%20Gartner.)
- ¹⁷ <https://pmarketresearch.com/it/web-3-0-decentralized-identities-dids-market>
- ¹⁸ https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf?utm_source=substack&utm_medium=email