UNDERGRADUATE LAW REVIEW AT UC SAN DIEGO

AUDREY THOMPSON

Balancing Innovation and Transparency: How Financial Institutions are Regulating AI

ABSTRACT. Trust in financial institutions is essential to maintain because it forms the foundation of economic stability. Customers must be confident that their money and personal data are secure through transparency and disclosure of information to the customer about the system's processes. Laws like the Securities Act impose consequences for misleading investors about a company's inner workings or capabilities. The Gramm-Leach-Bliley Act (GLBA) ensures financial institutions inform customers of data collection and sharing practices, along with maintaining rigorous security measures. However, with the introduction of generative artificial intelligence models (GenAI) into financial services, risks for misuse and insufficient protection have increased. GenAI models and their decision-making processes are difficult to regulate under current disclosure requirements. To combat this, states have passed laws to minimize the risk of algorithmic discrimination and promote transparency. However, these measures are inconsistent, and while a federal AI privacy law is unlikely to pass, the industry can still streamline regulatory and compliance efforts by adopting common definitions of relevant terminology and expanding existing legislation to improve digital consumer data protections.

AUTHOR. Audrey W. Thompson is a third-year double major in Joint Math-Econ and Philosophy at UC San Diego. She is interested in risk management and regulatory compliance and wants to work as a data analyst before pursuing a J.D. She would like to thank her editors, Firdevs Dilekchi and Aadyant Suresh, along with her peer reviewer Professor J. Lawrence Broz, and the entire Undergraduate Law Review team, for their contributions and support throughout the writing process.

INTRODUCTION

Societies are built on the expectation of trust. People trust that their cars will drive safely, that their groceries will not contain poison, and that the government will protect their personal information. This implicit social trust allows people to organize at the state and federal levels. However, "social trust" is functionally identical to forced reliance because people must trust government-backed agents or opt out of society entirely. This is exemplified by the financial industry, where it is impossible to engage as an active member of society without a bank account, credit card, or some other relationship to a financial institution. Since individuals are required to trust financial institutions with highly sensitive, personally identifiable information (PII), the government is responsible for ensuring institutions act in the people's best interests.

Under the Gramm-Leach-Bliley Act (GLBA), financial institutions[1] are required to protect customers' non-public information (NPI), including their name, address, phone number, account balances, bank account and credit card numbers, date and location of birth, social security number, income and payment history, driver's license information, and tax return information.[2] Firms collect this information directly through customer disclosures and applications, or indirectly through transaction histories and consumer reporting agencies.[3]

Sensitive customer information has historically been protected through strict regulation of data collection and sharing practices, along with penalties for misconduct. Regulatory agencies like the Federal Trade Commission (FTC) ensure transparency through audits and enforced disclosures, such as customer notices and reporting data breaches.[4] The FTC serves as a broad check to prevent fraud and promote competition between businesses. However, the primary regulator of financial products and services is the Consumer Financial Protection Bureau (CFPB), which works in tandem with the FTC, often sharing information to work efficiently where

[1] Financial institutions are companies that offer consumers financial products or services like loans, financial or investment advice, or insurance.

[2] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, 6821-6827 (1999).

[3] Fed. Trade Comm., *Business Guidance Resources*, *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act* (July, 2002), https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.

[4] *Id.*

jurisdictions overlap.[5] Laws like the GLBA require firms to disclose when customer information is collected and shared, and where the information is shared. In practice, this disclosure is located within the terms and conditions page that customers read and accept before using a product.[6] Unfortunately, terms and conditions pages are dense and difficult to read, often hiding clauses in the fine print. Additionally, firms must allow customers to opt out of sharing NPI with non-affiliated third parties,[7] except under special circumstances.[8]

The financial industry requires extraordinary access to customer information to function. Institutions managing sensitive data are held to a higher standard by the law, known as fiduciary duty.[9] The fiduciary has a responsibility to their client or beneficiary to follow certain duties: care, loyalty, good faith, confidentiality, prudence, and disclosure.[10] Corporate directors must possess and critically assess all material information reasonably available to them before making a decision, maintaining confidentiality, and acting with impartiality and absolute honesty.[11] These legal responsibilities are imposed because of the imbalance of trust and confidence between a client and the institution, as the client relies heavily on the institution's services. Institutions must take additional steps to ensure trust remains intact. The consequences of misusing or inadequately shielding NPIs in the financial industry are severe, leaving compromised consumers at risk of identity theft and fraud. This may require consumers to freeze credit, change passwords, and replace debit and credit cards.[12]

Traditional AI, like machine learning algorithms and neural networks, was

---

[5] Fed. Trade Comm., *Cooperation Agreements*, *FTC and CFPB Interagency Cooperation Agreement* (February, 2019), https://www.ftc.gov/legal-library/browse/cooperation-agreements/ftc-cfpb-interagency-cooperation-agreement.

[6] Fed. Trade Comm., *supra* note 3.

[7] Third parties are any entity outside of the umbrella organization and include contracted marketing or technology service providers for financial companies.

[8] 15 U.S.C. §§ 6801-6809, 6821-6827.

[9] Fed. Deposit Insurance Corp., *Banker Resource Center*, *Trust/Fiduciary Activities*, (June 27, 2025), https://www.fdic.gov/banker-resource-center/trustfiduciary-activities.

[10] Wex Definitions Team, *fiduciary duty*, L. Info. Inst. (March 2026), https://www.law.cornell.edu/wex/fiduciary_duty.

[11] *Id*.

[12] Baird Private Wealth Management, *So Your Data Has Been Leaked – Now What?*, https://www.bairdwealth.com/insights/wealth-management-perspectives/2024/11/so-your-data-has-been-leaked-now-what/ (last visited Feb. 16, 2026).

developed and made in-house by financial firms starting in the 1960s. In the 1990s, the introduction of neural networks sparked another boom.[13] OpenAI's 2022 release of ChatGPT kick-started the widespread implementation of generative artificial intelligence (GenAI), integrating AI Large Language Models (LLMs) into the financial industry.[14] Natural language processing models are used to scrape data to determine potential risks, and generative AI chatbots are used in customer service roles.[15] GenAI models have significantly more parameters than traditional AI models; this increased complexity has created issues for regulators in ensuring financial institutions meet explainability and interpretability requirements.[16] This "black box" inscrutability surrounding AI and its involvement in financial firms increases the risk of mishandling consumer information.

In the United States (U.S.), there are no federal privacy statutes directly addressing AI, leaving financial firms and regulators to rely on existing privacy laws. The Securities Act of 1933 and the Securities Exchange Act of 1934 (SEA) were passed to regulate financial fraud through periodic disclosures. The Chevron doctrine, established in *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.* (1984), gave federal regulatory agencies significant freedom to interpret statutes before it was overturned by *Loper Bright Enterprises v. Raimondo* (2024).[17] The Gramm-Leach-Bliley Act (GLBA), passed in 1999, also maintains privacy and safeguards rules for financial institutions, mandating considerable efforts be made to protect NPI. Third-party risks are a major concern for GLBA enforcement, as firms may share information with third parties that have inadequate privacy practices. This was demonstrated in an administrative settlement, when the FTC filed a complaint against Ascension Data & Analytics, LLC for engaging a third-party vendor that was non-compliant with GBLA standards.[18] Existing laws cannot protect financial NPI processed by AI systems, and new laws must be passed to adapt to the current technological landscape.

The European Union passed the EU AI Act in 2024, which took a

[13] Bonnie G. Buchanan, *Artificial Intelligence in Finance* (The Alan Turing Institute 2019).
[14] Tableau, *What is the history of artificial intelligence (AI)?*, https://www.tableau.com/data-insights/ai/history (last visited Feb. 7, 2026).
[15] U. S. Government Accountability Office, *Artificial Intelligence: Use and Oversight in Financial Services* (May 19, 2025), https://www.gao.gov/products/gao-25-107197.
[16] Regulatory compliance often involves providing understandable bases for decisions. When AI is used in those decision-making processes, their structure and function must be comprehensible to company management and regulators.
[17] Loper Bright Enters. v. Raimondo, 603 U.S. 369 (2024).
[18] Ascension Data & Analytics v. Pairprep, 105 F.4th 749 (5th Cir. 2024).

"human-centric" approach to regulation, serving as a blueprint for the Utah Artificial Intelligence Policy Act and the Colorado Artificial Intelligence Act, both passed in 2024.[19] The EU AI Act was the first comprehensive regulation on AI, banning the use of AI in biometric public identification and categorization, social scoring, facial recognition databases based on the internet or CCTV, and more.[20] The Act identifies and manages risk over different stages of AI development and deployment. The EU AI Act applies to all public and private AI systems used in the EU. Since the European market is very large, this could lead to even non-European companies adopting the EU's regulations to enter their market.[21] The U.S. has not followed in the EU's footsteps, opting instead to minimally supervise AI development and encourage speedy innovations.

While the U.S. federal government remains permissive, states have begun passing legislation to increase protections for financial data. However, this creates a patchwork of laws that can be confusing and expensive for companies to comply with compared to an overarching law. While a federal law would increase efficiency, it may result in the rollback of protections in several states, as federal law rarely contains robust protections. Standardizing terminology for AI models would help streamline compliance for companies and regulators alike, even without a federal privacy law. In the financial sector, where regulations are stricter, consistent definitions could increase efficiency, similar to a federal law, without overriding state regulations, and updating the GLBA to address modern technology could fill gaps in current legislation.

I. OVERVIEW OF U.S. PRIVACY LAWS

Privacy torts under common law involve publicly disclosing private information, appropriating someone's identity, or otherwise intruding on someone's privacy.[22] Courts also require proof of malice to sue consumer reporting agencies for privacy violations, as information is freely disclosed by the consumer and not openly available.[23] In the financial industry, security breach cases are class actions, and all 50 states require financial institutions to notify consumers, regulators, and news media

[19] Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689) 1.
[20] *Id.*
[21] *Id*.
[22] Stephen M. Bainbridge, *Corporate Law* (Saul Levmore et al. eds., 4th ed. 2020).
[23] *Id.*

when a breach occurs.[24] Transparency and disclosures are paramount to ensuring investor confidence, and statutes require financial institutions to provide full and accurate information about their information tracking and sharing practices.[25]

A. The Securities Act of 1933

The Securities Act of 1933 was enacted to regulate securities fraud, requiring annual audits by the Securities Exchange Commission (SEC).[26] The Securities Act imposed liability for misrepresentations or omissions of information in any written or oral statements connected to securities being sold.[27] For example, if registration statements included an untrue statement or omission, anyone who bought the security could sue for damages without proving the misrepresentation led to the purchase.[28] Most security fraud involves omissions in a firm's periodic disclosures, including audited financial statements and reports of yearly activities. Securities fraud results in eroded trust in financial markets, damage to the overall economy, and financial loss for investors.[29] This distorts the market, as damaged trust changes how investors allocate their capital. Substantive disclosure requirements present an issue for companies using generative AI LLMs because many models are "black box"[30] systems whose processes are difficult to understand or explain.[31] This inscrutability means models behave unintuitively, and developers cannot follow the decision-making process.[32] Unlike machine learning algorithms and traditional AI, GenAI is more complex, with more parameters affecting the output.[33] This impacts explainability because as the number of

---

[24] Privacy Rights Clearinghouse, *Data Breach Notification Laws: A 50-State Survey (2026 Edition)*, (Jan. 28, 2026),
https://privacyrights.org/resources-tools/reports/data-breach-notification-laws-50-state-survey-2026-edition.

[25] *Id.*

[26] Wex Definitions Team, *Securities Act of 1933*, L. Info. Inst. (Oct. 2023),
https://www.law.cornell.edu/wex/securities_act_of_1933.

[27] Bainbridge, *supra* note 22.

[28] *Id.*

[29] *Id.*

[30] Black box AI are systems whose internal processes are unknown to the user. Users can only perceive the input or output and have no conception of how the AI produced the output.

[31] Tom C.W. Lin, *Artificial Intelligence, Finance, and the Law,* 88 Fordham L. Rev. 531 (2019).

[32] Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines,* 87 Fordham L. Rev. 1085 (2018).

[33] *Id.*

variables increases, it becomes progressively harder to connect changes in the output to individual variables.[34]

Currently, the SEC is combating "AI-washing," when companies overstate or fabricate the use or capabilities of AI in their products to make them more appealing to investors. In 2024, the SEC settled charges against investment advisers Delphia (USA) Inc. and Global Prediction Inc. for AI-washing their products, resulting in civil penalties of $225,000 and $175,000.[35] According to the SEC order against Delphia, the company claimed to use client data to train AI to personalize investment advice for customers.[36] These false claims were made in the company's SEC filings, press releases, and on their website.[37] However, the SEC found that Delphia had not actually used client data or written any machine learning algorithm to use client data in its investment process.[38] Similarly, Global Predictions claimed to be the "first regulated AI financial advisor", using "AI-driven forecasts" in its technology.[39] However, the company was unable to provide documentation that these claims were true, and further failed to disclose conflicts of interest from individuals giving testimonials about the AI's performance.[40] Global Predictions also falsely claimed its models outperformed International Monetary Fund (IMF) forecasts by 34%, and had $6 billion in assets on the platform, which was reported on the Form ADV.[41] AI-washing cases are likely to persist, including cases where the misleading claims are not as obviously false.

In 2023, the SEC proposed new rules to eliminate conflicts of interest for broker-dealers and investment advisors when using predictive data analytics like GenAI and machine learning.[42] These rules would prevent firms from using AI, which analyzes data to generate investment recommendations, to mislead prospective

[34] Andrew D. Selbst & Solon Barocas, *supra* note 32.
[35] U.S. Sec. and Exch. Comm'n, *SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence* (Mar. 18, 2024), https://www.sec.gov/newsroom/press-releases/2024-36.
[36] *Delphia (USA), Inc.,* Respondent, No. 3-21894 (Mar. 18, 2024).
[37] *Id.*
[38] *Id.*
[39] *Global Predictions, Inc.*, Respondent, No. 6573 (Mar. 18, 2024).
[40] *Id.*
[41] *Id.*
[42] Press Release, *U.S. Sec. and Exch. Comm'n, SEC Proposes New Requirements to Address Risks to Investors From Conflicts of Interest Associated With the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers* (July 26, 2023), https://www.sec.gov/newsroom/press-releases/2023-140.

investors about their potential success.[43] Firms would also be required to maintain documentation of written policies and procedures to remain compliant with the rules in an effort to tackle the "black box" concern of AI models.[44] However, the SEC withdrew this proposed regulation in 2025, under SEC Chair Paul Atkins.[45] AI-washing in the financial industry distorts competition by artificially inflating the stock prices of deceptive firms and eroding consumer and investor confidence. This underscores the need for transparency around AI usage and ability.

B. Chevron U.S.A., Inc. v. NRDC and Loper Bright Enterprises v. Raimondo

In 1977, Congress amended the Clean Air Act (CAA) to ensure states met the Environmental Protection Agency's (EPA) national air quality standards. However, the amended act did not include a specific definition of "stationary source" for pollution-emitting devices in a new permit program regulating the modification of stationary sources.[46] Under EPA regulations, existing plants could install or modify equipment without meeting standards so long as the modifications did not increase total emissions.[47] The "bubble concept" interpreted a "stationary source" as a whole plant, including the individual pollution-emitting devices.[48] An alternative interpretation identifies each device as a stationary source and prevents modifications of equipment that increase its individual emissions.[49] The Chevron doctrine was established in *Chevron U.S.A., Inc. v. NRDC* (1984), after the EPA used a plantwide definition of "stationary source" under the CAA.[50] The Court held that unless Congress or legislative history directly addressed the issue at hand, reasonable agency interpretations were automatically accepted in ambiguous cases.[51]

The Chevron doctrine established a two-step framework. If Congress directly addressed the issue, then the Chevron doctrine did not apply, and the court and agency

---

[43] Press Release, U.S. Sec. and Exch. Comm., *supra* note 42.
[44] *Id.*
[45] U.S. Sec. and Exch. Comm'n, *Rules and Regulations*, *Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers* (June 12, 2025), https://www.sec.gov/rules-regulations/2025/06/s7-12-23.
[46] Chevron v. Natural Resources Defense Council, 467 U.S. 837 (1984).
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*

deferred to Congress.[52] If congressional intent was unclear or ambiguous, courts evaluated whether the agency's interpretation of the statute was "permissible" and were required to accept the interpretation regardless of whether they agreed.[53] Agencies' interpretations were given greater power and flexibility, allowing them to quickly adapt to innovations in fast-moving industries.

However, in 2024, the Chevron doctrine was overturned by the decision in *Loper Bright Enterprises v. Raimondo* (2024), which asserted that courts were responsible for interpreting constitutional and statutory provisions.[54] This shifted power back to the courts, which no longer had to consider agencies' interpretations in their rulings. Courts were given discretionary authority to fill statutory gaps and determine the correct interpretation. While agency interpretations may still influence a court's reading, they are no longer automatically accepted.

In *Chevron,* the argument for agency interpretation was based on technical expertise and the belief that an administrative body responsible for enforcing the statute would be better positioned to consider all interests.[55] The allowance for agency interpretation gave federal regulators greater flexibility when identifying and monitoring violations. Financial technology (fintech) products and AI systems are not considered financial institutions under GLBA definitions, and once on the market, they are reviewed and reworked at lightning speed.[56] A greater degree of flexibility makes a significant difference in federal agencies' ability to adapt and enforce regulations.

Despite legislative changes, the FTC and the CFPB released a statement emphasizing their commitment to monitoring AI systems and holding companies accountable for fraud.[57] This will increase the rules set by regulators to fill administrative gaps no longer covered by liberal enforcement interpretations. Additionally, states will legislate AI privacy, creating a patchwork of laws. Adaptability is extremely important for both companies and regulators, and the government should

---

[52] *Chevron*, 467 U.S. 837.

[53] *Id.*

[54] Loper Bright Enterprises v. Raimondo, Secretary of Commerce, 603 U.S. 369 (2024).

[55] *Chevron*, 467 U.S. 837.

[56] Ally Heinrich, *Failing Fast: Why It's Essential for Entrepreneurs*, Harvard Business School: Business Insights Blog (April 3, 2025), https://online.hbs.edu/blog/post/fail-fast.

[57] Press Release, FTC Chair Khan and Officials from DOJ, CFPB and EEOC Release Joint Statement on AI (April 25, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-chair-khan-officials-doj-cfpb-eeoc-release-joint-statement-ai.

take steps to clarify regulations. The more ambiguity, the easier it is for bad actors to take advantage of consumers.

C. The Gramm-Leach-Bliley Act

Another privacy standard commonly used in the financial industry is the Gramm-Leach-Bliley Act, which is comprised of the Privacy Rule and the Safeguards Rule.[58] The Privacy Rule requires financial institutions to provide customers with annual notices of information collection and sharing practices and allow customers to opt out of sharing NPI with non-affiliated third parties.[59] A non-affiliated third-party refers to any entity outside of the umbrella organization, including consultants, service providers, auditors, or other companies with which the financial institution may have a contracted vendor relationship.[60] Firms are not required to allow customers to opt out of sharing information with third parties performing essential functions for the business, such as processing transactions or complying with legal requirements.[61] Annual disclosures are not required if the institution does not share information with third parties and has not changed its privacy policy.[62] The Privacy Rule does not limit the sharing of NPI with third parties; it only requires that the customer be notified.[63]

The Safeguards Rule maintains robust information security programs at financial institutions.[64] These programs must meet five requirements: (1) the institution must retain employees whose primary responsibility is coordinating the security program, (2) it must be able to accurately identify what most reasonable risks to customer information are, (3) the team must design and implement safeguards against all identified risks, (4) the program must be subject to federal oversight, and (5) it must regularly undergo evaluations and improvements.[65] Customers and the FTC are also required to be notified no later than 30 days after discovery[66] of any data breaches or

[58] 15 U.S.C. §§ 6801-6809, 6821-6827.
[59] *Id.*
[60] Wex Definitions Team, *15 U.S. Code § 6809 - Definitions*, *Nonaffiliated Third Party*, L. Info. Inst. (Nov 1999), https://www.law.cornell.edu/uscode/text/15/6809#5.
[61] 15 U.S.C. §§ 6801-6809, 6821-6827.
[62] *Id.*
[63] Fed. Deposit Insurance Corp., *Bank Examinations*, *Privacy Rule Handbook* (Aug. 11, 2023), https://www.fdic.gov/bank-examinations/privacy-rule-handbook.
[64] 15 U.S.C. §§ 6801-6809, 6821-6827.
[65] Dee Pridgen, *Consumer Protection Law in A Nutshell* (Jesse H. Choper et al. eds., 5th ed. 2020).
[66] Discovery refers to the moment a company finds a "notification event" or security breach involving the unauthorized acquisition of 500+ consumers' unencrypted information.

leaks containing the NPI of at least 500 consumers.[67] The FTC enforces Safeguards Rule violations. The FTC investigates following data breaches and consumer complaints, and imposes financial penalties or lawsuits on financial institutions that fail to maintain adequate security measures.[68]

In 2025, the FTC settled with Cleo AI Inc., an online cash advance company promising customers instant cash payments of up to $250.[69] According to the FTC complaint, Cleo AI misled consumers about the amount of money and the speed of delivery, as well as making it unnecessarily difficult to cancel subscriptions.[70] Cleo AI agreed to pay $17 million to settle the allegations that it had misrepresented its services to consumers and failed to provide simple methods to stop recurring payments.[71] The FTC defined "financial institutions" broadly, including any entities "significantly engaged" in providing financial products or services.[72] The FTC reinforced that "finders," entities connecting consumers with non-traditional lenders like Cleo AI, are included as financial institutions.[73] AI-driven tools require the same level of oversight as traditional financial institutions to prevent deception and will be treated as such.

D. Ascension Data and Analytics, LLC

Despite these precautions, determining when customer information is being mishandled is difficult, particularly when third-party vendors are attacked. Third-party systems are vulnerable to cybersecurity attacks, and firms must make efforts to secure the NPI shared with these processors, while continuously monitoring security practices.[74] In the case of Ascension Data and Analytics, LLC, the FTC found that Ascension engaged a third-party vendor with security provisions that were not compliant with the GLBA, violating the Safeguards Rule.[75] This poses an issue to AI vendors since the prioritization of fast innovation in tech companies is antithetical to

[67] Fed. Trade Comm., *supra* note 3.
[68] *Id.*
[69] FTC v. Cleo AI, 2025 U.S. Dist. LEXIS 82589 (S.D.N.Y 2025).
https://www.ftc.gov/legal-library/browse/cases-proceedings/cleo-ai-inc-ftc-v.
[70] *FTC,* 2025 U.S. Dist. LEXIS 82589.
[71] *Id.*
[72] Fed. Trade Comm., *supra* note 3.
[73] *FTC,* 2025 U.S. Dist. LEXIS 82589.
[74] Jin-Wook Chang et al., *Cyber Vulnerabilities at Large US Financial Institutions and Their Third-Party Service Providers,* Finance and Economics Discussion Series 2025-103 (Nov. 2025),
https://www.federalreserve.gov/econres/feds/files/2025103pap.pdf.
[75] Ascension Data & Analytics, No. 192 3126 (Dec. 22, 2021).

the rigid privacy concerns and devastating consequences of failure to protect NPI.[76] The speed at which models are developed and released makes it unlikely that models are compliant without deliberate actions to enforce security.

Many financial institutions contract with LLMs and other GenAI models since they do not have the capability to build comparable models. Over time, financial giants may choose to build their own large language models (LLMs) to specialize and avoid privacy concerns, but smaller companies must continue to use third-party vendors to remain competitive. For instance, J.P. Morgan and Chase developed OmniAI, an in-house AI model that accelerates processes while maintaining necessary security.[77] Concerns arise from the use of public LLMs due to the uncertainty of whether sensitive information fed into the model is kept separate from its training data, erased, or stored. If NPI is stored within the model, malicious prompt engineers could cause models to disclose information inadvertently.[78] For example, people override ChatGPT's guardrails around sensitive conversation topics by masking the topic through roleplay.[79] At the 2023 Def Con conference, one hacker told an AI that his name was a credit card number, then asked for his name and received the number.[80] While corporate AI models are more complex than public AIs, they have more points of failure. Corporate AI models are connected to tools and databases which are more vulnerable to chain-of-thought hijacking, a form of cyberattack that hides the malicious input in innocuous reasoning and bypasses safety checks that struggle with longer reasoning sequences.[81] These cyberattacks abuse the AI's objective of solving reasoning puzzles and minimize the model's attention towards the actual instructions.[82] In recent testing, chain-of-thought hijacking has had a success rate between 94-100% on Gemini 2.5 Pro, Gpt o4 mini, and Claude 4 Sonnet.[83] AI

[76] U. S. Government Accountability Office, *supra* note 15.

[77] Gizel Gomes, *AI in Banking: JP Morgan Leads the AI Sphere*, CTO Magazine (Sep. 3, 2024), https://ctomagazine.com/jp-morgan-chase-accelerates-ai-adoption/.

[78] Malicious prompt engineering, also called prompt injection, is a cyberattack where prompts are designed to manipulate LLMs into ignoring preset guardrails. It is considered the top security risk for LLM applications as of 2025.

[79] Shannon Bond, *What happens when thousands of hackers try to break AI chatbots*, National Public Radio (Aug. 15, 2023, 5:01 AM), https://www.npr.org/2023/08/15/1193773829/what-happens-when-thousands-of-hackers-try-to-break-ai-chatbots.

[80] *Id.*

[81] Jianli Zhao et al., *Chain-of-Thought Hijacking* (Univ. of Oxford, Working Paper, 2025).

[82] *Id.*

[83] *Id.*

adoption is still outpacing organizations' ability to implement strong controls and safeguards. Respondents to Thoropass' 2026 State of Audit and Compliance Report viewed sensitive data exposure via AI tools, unapproved shadow AI use, and third-party AI vendor risk to be their top three AI-related risks, resulting in regulatory scrutiny.[84]

E. Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

President Biden defined Generative AI (GenAI) in Executive Order 14110 as a class of AI models that can produce derivative content from input data.[85] This is different from traditional AI, which is a machine learning algorithm developed by institutions. These models, used for pattern recognition tasks such as trading, credit underwriting, and process automation, are trained on less input data and are much less sophisticated than GenAI models.[86] Outputs are easier to explain because changes can be linked directly to the limited number of parameters.[87] President Biden indicated that GenAI models are more complex, require more computational power, and are prone to "hallucinations" where the model outputs fabricated information as "truth."[88] Since most financial institutions contract GenAI models, auditors may not have access to all necessary information to assess risks.[89] In a test run by Columbia Journalism Review on eight generative search tools, including ChatGPT and Gemini, hallucination rates ranged from 37-94% depending on the model.[90] Significant checks on the information delivered by AI must be instituted, especially in the financial domain, where decisions rely heavily on the precision of information.

Corporations apply human oversight as a check on AI decision-making. This

---

[84] Thoropass, *2026 State of Audit & Compliance Report* (2026), https://info.thoropass.com/hubfs/2026-State-of-Audit-and-Compliance-Report.pdf.

[85] Fed. Reg., *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (Nov. 1, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[86] *Id.*

[87] *Id.*

[88] IBM, *What are AI hallucinations?*, https://www.ibm.com/think/topics/ai-hallucinations (last visited Feb. 24, 2026).

[89] U.S. Dep. of the Treasury, *Treasury Releases Report on the Uses, Opportunities, and Risks of Artificial Intelligence in Financial Services*, *News* (Feb. 8, 2025), https://home.treasury.gov/news/press-releases/jy2760.

[90] Jenna Ross, *Ranked: AI Hallucination Rates by Model*, Visual Capitalist (Nov. 27, 2025), https://www.visualcapitalist.com/sp/ter02-ranked-ai-hallucination-rates-by-model/.

addresses potential issues with AI tools that reinforce biases and violate fair lending laws prohibiting discriminatory practices. For regulators, a person must be responsible for important decisions to enforce accountability for undesired outcomes. The EU AI Act defines important decisions as those that have significant impacts on people's safety and fundamental rights.[91] According to the CFPB in 2016, institutions using AI are responsible for ensuring that their applications align with legal standards and do not unintentionally include protected categories or proxies to predict creditworthiness and other consumer lending practices.[92] Assigning responsibility to financial institutions for AI misuse incentivizes them to mitigate bias and improve model transparency.

F. Current AI Legislation

In 2025, President Trump passed Executive Order 14365 on Ensuring a National Policy Framework for Artificial Intelligence to "remove barriers to and encourage adoption of AI applications across sectors."[93] The Order specifically concerns commerce and U.S. economic dominance.[94] Historically, the U.S. has been "hands-off" in regulating new technology, similar to Executive Order 14365. The Order requests that federal agencies override stringent state laws to give U.S. companies the ability to freely innovate with AI models to establish global supremacy and a commercial edge.[95] President Trump is primarily concerned with the issues associated with overregulating AI use rather than the risks of implementing unsafe AI. This may compromise consumers' private data as AI is adopted faster than laws can be developed. AI is a powerful tool, and the industry must proceed with a human-centric approach to ensure it does not create widespread bias, leak significant amounts of consumer data, or invade privacy through unauthorized surveillance.

At the forefront of AI regulation is the European Union, which passed the EU AI

---

[91] Artificial Intelligence Act, art. 5.

[92] Bureau of Consumer Financial Protection, *Compliance Bulletin and Policy Guidance* (Oct. 31, 2016), https://files.consumerfinance.gov/f/documents/102016_cfpb_OfficialGuidanceServiceProviderBulletin.pdf.

[93] *Ensuring a National Policy Framework for Artificial Intelligence*, The White House (Dec. 11, 2025), https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

[94] *Id.*

[95] The White House, *White House Unveils America's AI Action Plan* (July 23, 2025), https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/.

Act in 2024, a global standard for AI governance.[96] The AI Act classifies AI by its level of risk and outlines specific regulations for minimal risk, limited risk, high risk, and unacceptable risk levels.[97] Most regulations and transparency obligations apply to high-risk systems, which include systems used to profile individuals, evaluate creditworthiness, and conduct risk assessments.[98] Developers of high-risk AI are required to establish risk and quality management systems, conduct data governance and extensive testing to ensure robustness, keep technical documentation and record-keeping for their models, provide instructions for operation, and maintain comprehensive human oversight.[99] Maintaining human oversight includes retaining at least two people who can fully understand the AI's limitations, address any anomalies, accurately interpret model output, and stop the system from operating at any point.[100] These regulations also require technical documentation and record-keeping, including programming models to automatically record events where the AI may present a risk, such as situations affecting people's safety, health, and privacy.[101] These records must log the period of time, reference database, input data, and people involved in verifying the model output.[102] The Brussels Effect, where international companies adopt EU regulations in order to access their market, would allow the EU AI Act to serve as a robust, generally adopted standard by companies using AI to maintain a consistent system.[103]

Several states, such as Colorado, Utah, and California, have already passed AI legislation emulating the EU AI Act, focusing on transparency and minimizing algorithmic discrimination.[104] In 2024, Colorado passed Consumer Protections for Artificial Intelligence, a law addressing the risks of algorithmic discrimination in high-risk AI systems.[105] Colorado used the same definition for AI as the EU AI Act: a high-risk system involving the use of AI in consequential decisions concerning the

[96] Artificial Intelligence Act, art. 5.
[97] *High-Level Summary of the AI Act*, EU Artificial Intelligence Act (Feb. 27, 2024), https://artificialintelligenceact.eu/high-level-summary/.
[98] *Id.*
[99] *Id.*
[100] Artificial Intelligence Act, art. 14.
[101] *Id.*
[102] Artificial Intelligence Act, art. 12.
[103] Anu Bradford, *The Brussels Effect* (online edn, Oxford Academic, 2020).
[104] Nat. Conf. of State Leg., *Artificial Intelligence 2025 Legislation* (July 10, 2025), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation.
[105] Consumer Protections for Artificial Intelligence, Colo. S.B. 24-205, Reg. Sess. (2024).

consumer.[106] The Colorado law mandates transparency and human oversight, implementing annual risk assessments, and requiring that customers be notified of which decisions will be made using AI.[107] Consumers are also allowed to appeal to a human review if the decision is harmful.[108] This includes being denied loans or otherwise deemed a high credit risk by AI due to associations with certain protected groups. Companies must disclose any foreseeable risks of algorithmic discrimination to the attorney general within 90 days of discovery.[109] Along with disclosure, companies are also required to use reasonable care to protect consumers from these risks.[110]

Utah enacted the Utah Artificial Intelligence Policy Act (UAIP), requiring companies to disclose when customers are interacting with generative AI.[111] This differs from other AI legislation, focusing on customer-facing AI rather than the use of AI in internal decision-making processes. The UAIP has similar disclosure requirements to the GLBA Privacy Rule, except that it specifically includes generated AI content.[112] Financial institutions that use chatbots or AI content fall into the category of "regulated occupations," or jobs that require state certifications to perform.[113] Under UAIP regulations, these occupations must "prominently" disclose generative AI use before beginning communication with a customer.[114] "Prominent" disclosure means that the customer must immediately be told that they are interacting with an AI at the start of the meeting, and the statement cannot be hidden in fine print on a website or otherwise.[115] This is important in maintaining the privacy of information because customers may change their behavior depending on whether they believe they are speaking with a human or an AI, and whether they believe their responses are being recorded and used for training. Employees of financial firms who use AI models may be advised to encrypt sensitive data or withhold it altogether to reduce data security risks.[116] However, average customers may be less cautious about

[106] Colo. S.B. 24-205.
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] Artificial Intelligence Amendments, Utah S.B. 149, Gen. Sess. (2024).
[112] *Id.*
[113] *Id.*
[114] *Id*.
[115] *Id.*
[116] FINRA, *Rules & Guidance, FINRA Reminds Members of Regulatory Obligations When Using Generative Artificial Intelligence and Large Language Models* (June 27, 2024), https://www.finra.org/rules-guidance/notices/24-09.

this due to a lack of adequate guidance on what is harmful to disclose. Consumers' lack of knowledge surrounding AI and its capabilities leaves consumer data at high risk of exploitation, necessitating regulations that protect data from leaks and breaches.

II. POTENTIAL SOLUTIONS AND THEIR RAMIFICATIONS

According to the December 2025 Ramp AI Index, the finance sector was the second-highest adopter of AI technology, with 62% of U.S. businesses having a paid subscription or contract with AI companies.[117] AI technology significantly increases operational efficiency, requiring firms to adopt the technology to remain competitive.[118] According to JP Morgan, LLMs reduce fraud and account validation rejection rates, while improving and personalizing customer experiences.[119] However, federal privacy legislation has yet to regulate AI, and as states fill the void with a patchwork of laws and regulations, regulators must also rely on existing privacy statutes.

In the Treasury's AI Request for Information, several respondents raised concerns around gaps in GLBA protections, noting that although GLBA provides customers the ability to opt out of sharing non-public information (NPI) with non-affiliated third parties, there are still situations where it is legal for firms to share NPI without these regulations.[120] Exceptions include if the information is outsourced to third parties that perform an essential function, or for legal compliance, like responding to subpoenas.[121] One solution would be to strengthen the GLBA by switching from opt-out to opt-in, making consumer privacy the standard rather than allowing financial institutions to share data unless the customer explicitly says otherwise.

LLMs require large quantities of training datasets to function at a high level. If models have less training data, the resulting AI system may have a limited ability to

---

[117] Ara Kharazian, *Ramp AI Index*, Ramp, https://ramp.com/data/ai-index (last visited Jan. 14, 2026).
[118] Smarsh, *Nearly 8 in 10 Financial Services Firms View AI as Critical to Industry's Success, Finds New Report from Smarsh*, Dec. 12, 2024, https://www.smarsh.com/press-release/nearly-8-in-10-financial-services-firms-view-ai-as-critical-to-industrys-success-finds-new-report-from-smarsh.
[119] J.P. Morgan, *How AI Will Make Payments More Efficient and Reduce Fraud* (Nov. 20, 2023), https://www.jpmorgan.com/insights/payments/security-trust/ai-payments-efficiency-fraud-reduction#:~:text=J.P.%20Morgan%20has%20been%20using,analysis%2C%20when%20they%20need%20it.
[120] 15 U.S.C. §§ 6801-6809, 6821-6827.
[121] *Id.*

learn, leading to poor generalization, amplified bias, and increased hallucinations.[122] Additionally, models trained on recursively generated data—data produced by older AI models—typically degenerate and undergo "model collapse" where they "forget" the true, original data and become increasingly inaccurate.[123] This would be a problem for any use cases, but especially in finance, where the margins for error are small. However, implementing an "opt-in" feature for financial NPI is unlikely to affect LLMs, as public AI models are not trained on confidential information due to the risks of data leaks. Furthermore, companies like Anthropic, which created Claude, already follow opt-in policies regarding user data, and specialized private AI models have safeguards in place to ensure customer NPI is not used to train public models.[124] Thus, including an "opt-in" feature can maintain a stable user experience while protecting customer privacy with financial institutions.

A. A Stringent Federal AI Privacy Law

The EU passed the AI Act with the goal of it becoming a de facto standard, prioritizing consumer protection and providing guidance to firms on how to implement and assess AI models for safety and compliance. The U.S. would similarly benefit from standardization in passing a federal law regarding AI.[125] States are developing a patchwork of AI governance laws, which leads to financial firms being held to different standards depending on their location, creating logistical barriers to ensuring complete compliance for firms operating across states.[126] Smaller firms may not have the budget or manpower to examine 50 different regulatory frameworks and ensure fairness and safety in the company's actions to all the standards.[127] Many smaller firms use AI to compete with the scale of large companies, but with the increase in concerns around litigation and compliance costs, one third are likely to reduce AI use,

---

[122] Ilia Shumailov et al., *AI Models Collapse When Trained on Recursively Generated Data*, 631 Nature 755 (2024).
[123] *Id.*
[124] Anthropic, *Model Report* (Feb. 20, 2026), https://www.anthropic.com/transparency#:~:text=from%20AI%20feedback.-,Training%20Data,we%20generated%20internally%20at%20Anthropic.
[125] *High-Level Summary of the AI Act*, *supra* note 97.
[126] Jordan Crenshaw & Michael Richards, *Technology*, *The Hidden Cost of 50 State AI Laws: A Data-Driven Breakdown*, U.S. Chamber of Com. (Nov. 18, 2025), https://www.uschamber.com/technology/the-hidden-cost-of-50-state-ai-laws-a-data-driven-breakdown.
[127] *Id.*

and one fifth may stop using AI entirely.[128] Implementing a federal standard can protect consumers and maintain national cybersecurity by enforcing safety requirements for all firms.

The EU AI Act is stricter than any privacy law in the U.S., due to the EU's historical attitudes around governance. AI models like GPT-5, Claude 4.5 Opus, and Gemini Pro are currently at the top of the market and belong to U.S.-based companies.[129] In Executive Order 14365, President Trump expressed economic concerns about the implementation of overly stringent AI laws.[130] Limiting access to robust training datasets or removing the now private data they were originally trained on could severely handicap AI models' ability to reason and function at an intelligent level. Reducing the amount of training data available to models will lead to less accurate outputs and an increased risk of overfitting.[131] Increased regulation slows innovation and introduces additional safety measures for a more "human-centric" approach to AI. Staying at the forefront of AI innovation and subsequent economic and productivity growth is at odds with the maximal protection of customer data necessary to curtail security concerns.

In 2023, the National Institute of Standards and Technology (NIST) released its AI Risk Management Framework (NIST AI RMF), a collaborative opportunity for private and public organizations to evaluate the risk and implementation of AI services.[132] The framework is optional, although it is intended to improve trustworthiness and support current risk management efforts.[133] NIST AI RMF introduces a Core of four functions: (1) govern; (2) map; (3) measure; (4) manage.[134] Governance establishes a culture of risk management and makes sure that risk

---

[128] Crenshaw & Richards, *supra* note 126.

[129] *LLM Leaderboard - Comparison of Over 100 AI Models from OpenAI, Google, DeepSeek & Others*, Artificial Analysis, https://artificialanalysis.ai/leaderboards/models (last visited Jan. 12, 2026).

[130] *Ensuring a National Policy Framework for Artificial Intelligence, supra* note 93.

[131] IBM, *What is Overfitting?*, https://www.ibm.com/think/topics/overfitting#:~:text=To%20prevent%20overfitting%2C%20you%20can%20try:%20*,to%20assess%20the%20accuracy%20of%20the%20model (last visited Jan. 29, 2026) (overfitting occurs when models fit too closely to training data and can no longer make accurate predictions on test data).

[132] NIST, *Overview of the AI RMF*, https://www.nist.gov/itl/ai-risk-management-framework (last visited Jan. 16, 2026).

[133] *Id.*

[134] Elham Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1.0),* Nat. Inst. of Standards and Tech. (2023).

assessments are carried out regularly.[135] The map function identifies an AI system's purpose and potential negative impacts before proceeding with developing the model.[136] The measurement function provides guidelines for the metrics and methodology of AI risk assessment tools, which must be some form of objective, repeatable, or scalable test.[137] The management function plans for consistent monitoring and improvements after model deployment, along with the development of damage control plans to recover from possible incidents.[138] The NIST AI RMF serves as a starting point for companies to manage AI risk, although it is intended for a general audience and unlikely to meet the specifications of the financial industry.

While the NIST AI RMF presents a solid avenue for risk mitigation, the framework is voluntary and unlikely to be codified due to its constantly evolving nature. In the financial sector, the NIST AI RMF is unclear on how to manage stricter consumer privacy standards. Furthermore, a federal privacy law would have a broader scope than current state legislation. As seen in Executive Order 14365, the U.S. is taking a relaxed approach to AI regulation. Therefore, a federal law would likely fall between state protections regarding stringency. While a federal law would bring greater clarity to businesses and consumers, it would simultaneously roll back state consumer privacy protections. Since the goal is to prioritize the protection of consumer data and information, weakening state-level laws may be counterproductive.

B. Standardizing Definitions for AI Models in the Financial Sector

Regardless of how existing regulatory frameworks are strengthened, common, universal definitions of AI models and terminology are necessary. Suggestions for a common definition of AI models have been introduced in the Treasury's AI Request For Information (AI RFI), Organization for Economic Co-operation and Development (OECD), and the EU AI Act. The AI RFI defines AI models within President Biden's Executive Order 14110, calling GenAI "the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content."[139] OECD defines GenAI as "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate

[135] Tabassi, *supra* note 134.
[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] Fed. Reg., *supra* note 85.

outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."[140] The definition outlined in the EU AI Act is similar, marking AI systems' primary characteristics as machine-based, adaptive after deployment, and capable of generating outputs from inferences about the input.[141]

The OECD and EU have more robust definitions of AI, while the AI RFI definition is broad enough to encompass traditional AI and statistical models, which should not be regulated in the same way as GenAI. Regardless of whether these definitions become the standard, a consistent definition of AI models and other relevant terminology would streamline collaboration between government agencies, private companies, and the courts. A federal statute would also ease logistical barriers for financial firms with interstate operations, since they only need to understand and abide by one definition. Adopting a common definition of AI achieves many of the same benefits as a federal privacy law without sacrificing strict state protections.

C. Overhauling GLBA

In 2025, the U.S. House Committee of Financial Services requested public feedback on consumer privacy laws, primarily Title V, Subtitle A of the GLBA.[142] This section contains the Privacy Rule, requiring financial institutions to give notice of their privacy policies and the opportunity to "opt-out" of disclosing consumers' NPI to unaffiliated third parties.[143] The House asked whether amending the GLBA was sufficient, if the definition of personally identifiable financial information (PII) and non-public personal information (NPI) should be expanded, if the definition of a financial institution should be expanded, and whether incentives to minimize data collection to the bare essentials were needed.[144]

Amending the GLBA could include expanding the PII definition to cover digital information like one's IP address, geolocation, behavioral analytics, metadata, and

---

[140] *OECD AI Principles overview*, OECD.AI, https://oecd.ai/en/ai-principles (last visited Feb. 2, 2026).
[141] Artificial Intelligence Act, art. 3.
[142] Press Release, House Committee on Financial Services Chairman French Hill (AR-02) and Subcommittee on Financial Institutions Chairman Andy Barr (KY-06), House Financial Services Committee Requests Feedback on Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals (July 31, 2025), https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=410833.
[143] 15 U.S.C. §§ 6801-6809, 6821-6827.
[144] Press Release, *supra* note 142.

other information inferred about the consumer from these tracking practices. This would better equip federal agencies to limit the sharing of modern data. A broader definition of NPI, which treats "consumers" and "customers" similarly, could standardize the application of privacy laws and create stricter protections for all types of data. Customers purchase a product or service from financial firms, while consumers are the end-users. Consumers differ from customers in business-to-business transactions, and by treating them similarly, consumer data will be better protected. Furthermore, including modern fintech apps and other entities that handle NPI in GLBA's definition of financial institutions could improve the consistency of protections across different entities.

Financial institutions should be restricted to collecting only the information necessary to carry out a given transaction, and be required to reduce the data retention period to minimize security risks. While requiring the deletion of outdated data reduces the risk of a data breach, additional safeguards and implementation practices may leave them more vulnerable to potential fraud. Financial institutions may be incentivised to oversee third-party vendors and improve protections by including a private right of action in the GLBA. If consumers are permitted to sue financial institutions for breaches rather than leaving enforcement exclusively to the FTC and other agencies, the number of lawsuits against financial institutions is likely to increase, leading firms to act more prudently when handling customer NPI. However, opening firms to customer lawsuits would increase their operational and legal costs. Overall, the GLBA should be updated in line with advancements in technology, regardless of whether it is considered sufficient to protect customer data from leaks.

CONCLUSION

Consumer data privacy is important in the financial industry, where people are forced to trust financial institutions with highly sensitive personal information. Federal laws like the Securities Act and the Gramm-Leach-Bliley Act (GLBA) have been passed to balance this relationship. These laws ensure companies are held liable should they defraud investors or act carelessly with customer data. However, regulators are still working to catch up to developments in modern technology. The introduction of AI and fintech apps has enabled financial firms to operate more efficiently at higher levels of risk. Currently, AI regulations are haphazard as different states pass their own legislation, and federal agencies promote a hands-off approach. While a more cautious, human-centric approach would prioritize robust consumer data protection, the current administration has instilled a competitive attitude, instructing federal agencies

to strike down overly strict state laws that impede a company's ability to dominate in the global market. Given this, it is unlikely that a federal law addressing AI and data privacy will pass. However, within the financial industry, it is necessary to standardize common AI terminology in order to streamline compliance checks. An overhaul of GLBA is also in order as fintech apps expand the types of institutions that might handle sensitive data, and third-party concerns become ever more worrying. As AI models become progressively more complex and integrated into financial institutions, customer risk of fraud, data breaches, and algorithmic discrimination skyrockets. Therefore, it is of the utmost importance that the industry and its regulators adapt to this new environment and remain flexible for future changes. The fastest effective way to achieve this is through standardizing AI terminology between firms and regulators and updating the GLBA to address modern technological violations of its principles.