Hashed & Salted | A Privacy and Data Security Update
June 2023

Financial Services and AI: Regulatory Developments

Financial services providers are quickly adopting the use of artificial intelligence (AI) to streamline and optimize internal processes and to meet evolving customer demands for smarter and more convenient ways to access, spend, save and invest money. As a result, U.S. financial regulators and lawmakers have been paying increased attention to—and expressing concerns about—the use of AI in financial services.

AI Use Cases in Financial Services

The global AI financial services market size was $8.3 billion in 2019 and is expected to increase to $130 billion by 2027. *Business Insider* reported that 80% of banks are keenly aware of AI benefits and are implementing or planning to implement AI solutions—75% of respondents at banks with more than $100 billion in assets are currently implementing AI strategies, compared with 46% of banks with less than $100 billion in assets. Additionally, the World Economic Forum and the Cambridge Centre of Alternative Finance's survey of 151 financial institutions in 33 countries reported that a large number of financial institutions are becoming mass adopters of AI and are using AI solutions as a business driver. The key survey findings noted:

- 85% of financial services providers are currently using AI in some form.
- 77% believe AI will become essential to their business in the next two years.
- 64% will be mass adopters of AI in the next two years.
- 52% have created AI-enabled products and services.
- 50% believe AI will be a competitive threat as others enter the market.

Rapid adoption of AI is revolutionizing the financial services industry by increasing the efficiency, accuracy and speed of financial services in numerous use cases. Financial services providers are employing AI for several tasks, including the following four use cases:

1. **Automating processes.** AI can automate repetitive tasks and processes, such as data entry and analysis, to reduce the amount of money and time and the number of errors associated with completing these tasks.
2. **Improving decision-making.** AI can utilize machine learning algorithms that are trained to analyze large data sets and identify trends or other indicators that can be used in making informed decisions about factors such as credit risk.
3. **Enhancing customer experience.** AI can improve customer service by providing personalized recommendations and advice. For example, AI-powered chatbots can answer questions, provide personalized investment advice, and use natural language processing and voice analytics to manage customer interactions without human assistance.
4. **Fraud detection.** According to *Insider Intelligence*, online payment fraud losses are expected to reach

$48 billion this year. AI can identify trends and patterns in online banking activity that usually go unnoticed by people.

These kinds of AI-driven processes are modernizing internal processes, improving the customer experience and increasing cost savings. In fact, *Insider Intelligence* reported that cost savings associated with implementing AI-driven processes in financial services will reach an estimated $447 billion by the end of this year. Given the benefits and associated cost savings, the trend toward mass adoption of AI in financial services is expected to continue. Naturally, regulators are taking notice and seeking to understand the implications of the use of AI in the financial services space.

Federal Regulatory Developments

AI and Financial Services

In the past two years, U.S. financial regulators have expressed significant interest in the use of AI in financial services. As an example, on March 29, 2021, the Board of Governors of the Federal Reserve System, the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation, the National Credit Union Administration and the Office of the Comptroller of the Currency jointly issued a request for information (RFI) on financial institutions' use of artificial intelligence. The RFI sought information to help the regulators understand the challenges and opportunities of AI with respect to governance, risk management and controls, and any challenges related to the development, adoption and management of AI.

In May 2022, the CFPB published a circular to address adverse action notice requirements of the Equal Credit Opportunity Act, which prohibits discrimination against credit applicants, and to advise that the requirements "apply equally to all credit decisions, regardless of the technology used to make them," including AI, and accordingly "do not permit creditors to use complex algorithms when doing so means they cannot provide the specific and accurate reasons for adverse actions [such as declined applications]." In the CFPB's most recent annual report, which details credit reporting agency (CRA) complaints, the CFPB directly addressed consumer harm that results from CRAs' reliance on AI-automated processes to screen and respond to consumer inquiries and requested that CRAs consider the burden on and potential harm to consumers.

In June 2022, the American Data Privacy Protection Act (ADPPA)—the first bipartisan, bicameral federal privacy bill—was introduced in Congress. The bill passed House committee markup with near unanimity, but it faced difficulty in the Senate, and no action was taken before the end of the 117th congressional term. If passed, the ADPPA would require greater transparency in the collection, use and sale of consumer data; provide minimum safeguards for data protection; and require management oversight of data privacy and security. The draft ADPPA also includes provisions that prohibit discrimination and require AI Data Privacy Impact Assessments. Given the January 2023 shift in the Senate's balance of power, it will be interesting to see how the ADPPA legislation unfolds.

More recently, at the end of 2022, the Biden administration issued a nonbinding policy document dubbed the "AI Bill of Rights." While the AI Bill of Rights is not specific to financial services, it provides instructive guidance on five fundamental rights that should be considered in the development of policy and use of AI in all industries:

1. Safe and effective systems
2. Algorithmic discrimination protections
3. Data privacy
4. Notice and explanation
5. Human alternatives, consideration and fallback

At a high level, the regulatory reviews and proposed legislation indicate that the implications of using AI in financial services are multifaceted and extensive, as they intersect with key legal issues such as anti-discrimination, regulatory compliance, automated decision-making, contracts, and intellectual property rights. Of course, one of the hot-button issues continues to be the privacy and security of financial data, which has been at the forefront of regulatory reviews and recently enacted or pending legislation.

Financial Data Privacy

Regulators are increasingly expressing concerns about the use of AI in financial services due to the heightened

information privacy and cybersecurity risks, given that AI provides financial services providers with exponentially greater abilities to collect and analyze consumer data. Regulators want to ensure that companies utilizing AI are properly using and protecting consumer data. Some recent regulatory developments in financial data privacy include the following.

Gramm-Leach-Bliley Act (GLBA) Safeguards and Privacy Rule Updates

In October 2021, the Federal Trade Commission (FTC) amended its Safeguards Rule, which requires banks and nonbank financial institutions such as fintech companies to implement information security safeguards. The amendments create prescriptive rules for issues such as encryption and multifactor authentication that apply to financial services providers. On Nov. 15, 2022, the FTC announced a six-month extension to comply with most provisions of its new Safeguards Rule. Covered "financial institutions" under the Safeguards Rule, which implements part of the GLBA, must now comply with the entire rule by June 9, 2023.

In Congress, the chairman of the House Financial Services Committee, Patrick McHenry (R-N.C.), introduced on Feb. 27, 2023, the Data Privacy Act of 2023, which would amend the GLBA to "modernize financial data privacy laws and give consumers more control over how their personal information is collected and used."

Key highlights from the proposed Data Privacy Act of 2023 include:

- **Consent to use nonpublic personal information (NPI).** The bill mandates that it is unlawful for financial institutions to willfully use NPI without the consent of an individual with whom the financial institution maintains a customer or consumer relationship.
- **Obligations for the collection and disclosure of data.** The bill requires financial institutions to disclose to individuals when their NPI or account credentials are being collected or shared and to notify nonaffiliated third parties when a consumer or customer has ceased sharing their data. The nonaffiliated third parties must also cease sharing the individual's data.
- **Privacy policy disclosure obligations.** The bill expands the requirements for information to be included in a financial institution's privacy policy disclosure.
- **Preemption.** The bill authorizes the states to expand protections over federal law if appropriate and requires preemption and a national standard that is set to supersede any state law.
- **Updates to the definition of a financial institution.** Financial institutions including bank and nonbank financial institutions such as fintech companies are already covered by the GLBA. The bill expands the definition of financial institutions to also include data aggregators.

Access to Financial Data—Open Banking Rule

The CFPB is working on a final proposal for its open banking rule. If codified, the open banking rule will enable consumers to own, access and share their financial data however and with whomever they choose. Open banking generally refers to a consumer's ability to control their financial data by allowing third-party financial services providers to access financial data in real time through the use of application program interfaces. The aggregation of a consumer's financial data provides a financial overview of the consumer, which financial services providers and fintech companies can use to tailor services, recommend products and improve consumer experiences. Consumer privacy and data security protections have been primary concerns related to open banking, and the CFPB sought public feedback on how to address these concerns, among others. The CFPB reported that it would issue a report in the first quarter of 2023 about public comments it received, which were due on January 25, 2023, although it has not yet done so.

What Companies Should Be Doing to Get Ready for AI and Financial Data Privacy Regulation in 2023

As both federal government and state officials continue to enact legislation throughout the U.S. that impacts the use of AI tools and financial data privacy, companies should:

- **Assess.** Review (i) the company's use of AI tools, and consider whether the tools and use are covered by applicable law; (ii) ensure all company practices surrounding the collection, usage, storage or transmission of financial data are compliant with applicable federal and state laws; and (iii) if the assessment identifies risks, identify and implement risk controls (technical, contractual, organizational).
- **Audit.** Conduct bias audits of AI tools, or ensure that third-party vendors are conducting such analyses. While these analyses are not required by all laws, financial services providers are likely subject to some anti-discrimination laws and should ensure that programs they use are not running afoul of those laws.
- **Know Your Data.** Assess what personal data you collect; why you collect it; how you collect, use and store it; and whether and how you share or provide access to it. This will aid your company in quickly responding to regulatory requests or changes.
- **Protect Your Data.** Ensure that your company has appropriate policies and security measures in place to protect the collected and processed data as required by applicable federal and state laws.
- **Write.** Be sure that your company has clear written policies that address the procedures for collection, storage, use, transmission and destruction of data and the use of AI.
- **Communicate.** Be sure to (i) notify all individuals about the use of AI tools where required by applicable law and/or (ii) notify all individuals about your data collection policy, including information about how this data will be secured to protect individual privacy interests.
- **Govern.** Be sure that company policies address the quality and integrity of data across the organization (data governance) and the integrity, accuracy, transparency, foreseeable risks, and social impacts of AI data sets and include a requirement for regular monitoring of AI systems to mitigate the potential of disparate and unfair outcomes (AI governance).
- **Consult.** Counsel is available to assist with risk assessment, policy development and training to ensure compliance with applicable laws and regulations.

Related Professional

Eyvonne Mallett . . . . . emallett@loeb.com

7296 REV1 06-13-2023