CENTER FOR DEMOCRACY & TECHNOLOGY

August 14, 2026

To: House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Re: Request for Information on AI Risks and Modernization in Financial Services

I. Introduction

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the House Committee on Financial Services's (Committee) request for information on the application of current federal laws and regulations related to the use of AI in the financial marketplace and any proposed reforms to provide for an appropriately modernized and comprehensive federal financial AI framework. CDT is a nonpartisan, nonprofit 501(c)(3) organization that works to advance civil rights and civil liberties in the digital age. CDT's work includes advocating for stronger governance of the use of AI affecting people's access to financial services.

CDT has called for stronger enforcement of laws and regulations and recommended reforms to promote accountability of AI integrated into the provision of financial services, housing, and related needs.[1] Our comments below:

- Suggest requirements to improve model fairness, explainability, and model risk management;
- Identify areas for improvement in existing financial data privacy laws and the limitations of disclosures alone as a governance measure;
- Discuss liability of financial institutions and their third-party service providers, and financial institutions' obligations to manage their third-party services; and
- Recommend steps to address AI's impacts on housing and workers.

[1] Center for Democracy & Technology, *Comment to Financial Regulators on Financial Institutions' Use of Artificial Intelligence Including Machine Learning* (Jul. 1, 2021), https://cdt.org/wp-content/uploads/2021/07/2021-07-01-CDT-Request-for-Information-and-Comment-on-Financial-Institutions-Use-of-Artificial-Intelligence-including-Machine-Learning.pdf; Center for Democracy & Technology, *Comment to House Financial Services Committee on Federal Consumer Financial Data Privacy Law* (Aug. 28, 2025), https://cdt.org/wp-content/uploads/2025/09/CDT-comment-on-federal-consumer-financial-privacy-law.pdf.

CENTER FOR DEMOCRACY & TECHNOLOGY

II. Model fairness, explainability, and model risk management (Responding to Questions 10, 11, 12, 16, and 17)

To ensure model fairness, explainability should be a prerequisite for AI deployment. Financial service and housing providers should not use AI systems for credit assessments and similar high-stakes tasks if they or their third-party service providers cannot articulate and explain the systems' inputs and design and how the systems' outputs are interpreted or otherwise affect decisions. Designing for explainability is vital because post-hoc explanations are less reliable for retracing the relationships that the system identified to produce its results.[2]

Explainability includes transparency to consumers before they are evaluated by an AI system and after the system has been used as part of the rendering of a decision. Prior to using AI to evaluate a consumer or otherwise assist in a decision, a provider should explain to the consumer why and how AI is used to make decisions about the provision of their services, and the type of personal data that will be processed by AI, to clarify how their AI use complies with relevant fair lending, fair housing, and consumer protection laws. Providers should explain to consumers the third-party sources of data for their AI uses and the third parties that will gain access to personal data through the AI uses. Applicants should be informed during the application process so they can determine whether to proceed with their applications before they have provided their data, determine whether any additional information is necessary to include in their applications, and verify that the data that will be considered is correct.

If an adverse decision is based in whole or in part on AI outputs, providers should be prepared to explain the reasons for denial and the processes for correcting any incorrect underlying data and appealing the decision. Such a requirement is already grounded in existing law: the Equal Credit Opportunity Act (ECOA) and Fair Credit Reporting Act (FCRA) require notices to applicants explaining the principal reasons for an adverse action or informing applicants of their right to request these explanations.[3] These disclosures are necessary for plaintiffs to vindicate their rights when a provider's use of an AI system aids in violating fair lending and other laws.

[2] Andrew D. Selbst and Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 Fordham L. Rev. 1085, 1113-15 (2018), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5569&context=flr.
[3] 15 U.S.C. §1691(d); 15 U.S.C. §1681(m).

Explainability should also be achieved through pre-deployment and post-deployment assessments of AI models.[4] When adopting an AI system, financial service and housing providers should obtain documentation from the developer explaining how the system's training data and design were evaluated, how the developer intends for the system to be used, and how the developer mitigated any identified risks.[5] Financial service and housing providers should conduct their own pre-deployment assessment to examine their data inputs and identify and mitigate any risks arising from any pre-training they conduct and their specific uses. Providers should continue monitoring the system's performance and impacts on a regular basis after deployment to surface and address any new or previously undetected risks.[6] However, without adequate in-house expertise and access to examine the systems, financial institutions might still require assistance from vendors to complete pre- and post-deployment assessments.

To ensure that pre- and post-deployment assessments are reliable and accurate, the assessments should be conducted by independent parties with sufficient access to the system, expertise to evaluate the system, and resources and capacity to complete a rigorous assessment.[7] Financial service and housing providers should make summaries of the methodologies and findings of their assessments available to regulators to demonstrate their compliance with existing fair lending and fair housing laws.

As the Committee observes, regulators replaced the superior Supervisory Guidance SR 11-7 with a weaker SR 26-2.[8] Regulators should restore SR 11-7, which provides more detailed guidance to help financial institutions manage model risks than SR 26-2 and can also help financial service providers work with their internal developers and third-party vendors to map data supply chains. SR 11-7's framework should inform financial service providers' use of generative AI and agentic AI models as well. It advises banks on managing risks in models developed in-house and in their third-party AI vendors. The guidance covers each stage of the

[4] Center for Democracy & Technology, *Comment to NTIA on AI Accountability*, at 25-29 (Jun. 12, 2023), https://cdt.org/wp-content/uploads/2023/06/CDT-comments-to-NTIA-on-AI-Accountability-53.pdf.
[5] *Id.* at 25-26.
[6] *Id.*
[7] Sasha Costanza-Chock, Inioluwa Deborah Raji, & Joy Buolamwini, *Who Audits the Auditors? Recommendations from a Field Scan of the Algorithmic Auditing Ecosystem*, 2022 ACM Conference on Fairness, Accountability, and Transparency (2022), https://dl.acm.org/doi/abs/10.1145/3531146.3533213.
[8] Federal Reserve Board and Office of the Comptroller of the Currency, *SR Letter 11-7: Supervisory Guidance on Model Risk Management* (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf; Federal Reserve Board, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation, *SR Letter 26-2: Supervisory Guidance on Model Risk Management* (Apr. 21, 2026), https://www.federalreserve.gov/supervisionreg/srletters/SR2602.pdf.

model lifecycle, from evaluating model design, logic, and training data, to documenting and continuously monitoring data inputs, performance, and corrective actions. It advises banks to assess and document the data quality and relevance of model training data, and to maintain inventories describing the types and sources of data inputs, outputs, and underlying components of each model. Instead of the approach taken by 26-2 to narrow this guidance, SR 11-7 should be explicitly extended to nonbank financial service providers, including AI companies providing consumer financial products and services.

SR 11-7 and the National Institute of Standards and Technology's AI Risk Management Framework (NIST AI RMF) can be treated as complementary frameworks. The NIST AI RMF provides guidance that is generally applicable across sectors, along with supplementary resources, to help companies improve explainability of their AI systems.[9]

III. Data privacy and disclosures (Responding to Questions 13, 14, 15, and 18)

One of the main laws specifically intended to govern privacy for financial services is the Gramm-Leach-Bliley Act (GLBA), which needs improvements to better achieve this objective.[10] GLBA aims to protect consumers' nonpublic personal information by restricting financial institutions from sharing consumers' financial data with nonaffiliated third parties without first notifying consumers and giving consumers the opportunity to opt out. GLBA's definitions of "financial institution" and "nonpublic personal information" should be clarified to ensure the statute covers data processed by or used to train AI systems used for financial services.

Steps that should be taken by Congress

There are a variety of steps Congress can take to improve banking laws. For instance, GLBA defines "financial institution" as any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Sec. 4(k) of the Bank Holding Company (BHC) Act.[11] Sec. 4(k) of the BHC Act lists a few examples of financial

[9] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework* (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[10] This section captures the gaps in GLBA and key necessities for an effective financial privacy framework discussed in CDT's August 2025 comments to the Committee. See Center for Democracy & Technology, *Comment to House Financial Services Committee on Federal Consumer Financial Data Privacy Law* (Aug. 28, 2025), https://cdt.org/wp-content/uploads/2025/09/CDT-comment-on-federal-consumer-financial-privacy-law.pdf.
[11] 15 U.S.C. §6809(3).

activities and factors to determine whether an activity is financial in nature.[12] These provisions and the illustrative examples in GLBA regulations suggest that providers of technological means to deliver financial services are subject to GLBA.

However, if an activity is not enumerated in the BHC Act or its regulations, then the factors for determining whether it is deemed financial hinge on the role it plays in delivering financial services. GLBA regulations provide a circular definition for "financial product or service," describing it simply as any product or service that could be offered by engaging in an activity under Sec. 4(k) of the BHC Act.[13] This definition leaves it up to the Board of the Federal Reserve System, in consultation with the Treasury Department, to designate financial activities that affect the scope of companies covered by GLBA.[14] GLBA should be amended to clarify that technology companies and data brokers that are increasingly accessing, processing, and disclosing financial data are financial institutions under GLBA.

In addition, GLBA defines "nonpublic personal information" as personally identifiable financial information a financial institution obtains directly from a consumer or by providing a financial product or service to the consumer.[15] However, GLBA regulations do not elaborate on the meaning of "personally identifiable financial information" other than to offer examples and to exclude information that does not identify a consumer and lists of names and addresses of customers of entities that are not financial institutions. GLBA should be amended to clarify that information that is "personally identifiable" identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or to a device that identifies or is linked or reasonably linkable to an individual. Clarifying these definitions will improve compliance with GLBA's notice-and-consent regime when data is shared for purposes related to AI.

However, while transparency is a necessary part of any privacy framework, a notice-and-consent model alone is insufficient to protect consumers from AI risks. When explanations of AI uses are buried within privacy notices, the burden is placed on consumers to digest all of the information provided regarding companies' AI uses and the personal data processed by their AI tools. The reality is that reading companies' lengthy privacy notices is

[12] 12 U.S.C. §1843(k)(3)-(4).
[13] 12 CFR §1016.3(m)(1).
[14] 12 U.S.C. §1843(k)(1)-(2); 12 CFR §1016.3(m)(1); 16 CFR §313.3(l)(1).
[15] 15 U.S.C. §6809(4).

unreasonably burdensome,[16] and they generally do not do so. Surveys in 2023 and 2024 found that the majority of consumers find privacy notices to be ineffective in informing them about companies' privacy practices or giving them control over their data, and want the government to do more to regulate companies collection and use of personal data.[17] In a 2021 survey, over 90% of consumers reported that they do not want financial institutions or fintech platforms to share their data for marketing purposes, 87% reported they want data collection to be restricted to only the data needed for a requested service, and 89% reported that the sharing of financial data should be subject to people's express opt-in.[18]

AI renders notice and consent less effective. AI products purport to improve the ability to predict the risk that a loan applicant will default or a rental applicant will violate their lease by analyzing greater volumes of data,[19] but without safeguards ensuring the accuracy and preventing the overcollection and misuse of financial and other personal data, AI can amplify risks of erroneous or discriminatory results from existing decision-making processes. As the financial services and housing industries increasingly adopt AI, third-party service providers will have greater incentives to incorporate the financial data they obtain into their own products in the absence of updated regulation to prevent abuse.

To more effectively address privacy risks from AI, relevant legal frameworks should center data minimization, which appropriately shifts the burden to companies who stand to gain from access to personal data at consumers' expense. Given that financial data collected and processed by financial service providers, housing providers, and third parties is highly personal, private, and sensitive, its collection and processing should be limited to only the extent that

---

[16] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society 540, 560 (2008), https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2013/02/Cranor_Formatted_Final1.pdf; Ryan Amos et al, *Privacy Policies Over Time: Curation and Analysis of a Million-Document Dataset*, In Proceedings of the Web Conference (2021), https://arxiv.org/pdf/2008.09159.

[17] Colleen McClain et al, *How Americans View Data Privacy*, Pew Research Center (2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/; Jana Arbanas et al, *Earning trust as gen AI takes hold: 2024 Connected Consumer Survey*, Deloitte (2024), https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html.

[18] Dan Murphy, David Silberman, & Stephen Arves, *Financial Health Network, Financial Data: The Consumer Perspective* 9-15 (2021), https://finhealthnetwork.org/wp-content/uploads/2021/04/Consumer-Data-Rights-Report_FINAL.pdf.

[19] Korin Munsterman, *When Algorithms Judge Your Credit: Understanding AI Bias in Lending*, UNT Dallas Law Review (2025), https://www.accessiblelaw.untdallas.edu/post/when-algorithms-judge-your-credit-understanding-ai-bias-in-lending-decisions.

such data is strictly necessary to effectuate a consumer transaction. For example, in contrast with GLBA, FCRA defines covered entities and covered data in a way that is clearly broader, includes purpose limitations that enumerate allowable data processing purposes, and gives consumers the right to have inaccurate or incomplete information corrected or deleted.

Steps that should be taken by regulators

Regulators can improve their interpretations of various statutory definitions in the GLBA, FCRA, and beyond. With respect to the meaning of "financial institutions," GLBA authorizes multiple agencies to enforce the statute with respect to the types of entities subject to each agency's jurisdiction, including the Federal Trade Commission (FTC). The FTC's authority does not extend to banks, savings and loan institutions, or federal credit unions, so the FTC enforces GLBA with respect to companies that are not among these types of institutions. GLBA regulations restrict FTC enforcement to only institutions that are *significantly* engaged in financial activities.[20]

The regulations offer examples to illustrate when companies are and are not "significantly" engaged in financial activities, but do not define this threshold. Several activities have been identified as financial in nature in the BHC Act regulations, including the provision of data processing, data storage, and data transmission services, facilities, and databases by any technological means if the data is financial, banking, or economic.[21] A company engaging in this activity could be subject to FTC authority generally, but the extent to which a company must engage in this activity to be subject to FTC enforcement of GLBA is unclear. Regulators should specify that companies that collect, process, and share consumers' financial data for purposes that materially affect consumers' use of financial services are significantly engaged in financial activities for purposes of FTC enforcement.

In addition, GLBA's definition of "nonpublic personal information" does not include publicly available information, which means publicly available information receives no protections, including that consumers cannot opt out of its sharing. The term is defined by regulations as any information that a financial institution has a reasonable basis to believe is lawfully made available to the general public from government records, widely distributed media, or legally required disclosures to the general public.[22] The regulations explain that a financial institution has a "reasonable basis" if the institution has taken steps to determine (1) that the information

[20] 12 CFR §1016.3(l)(3); 16 CFR §313.3(k)(1).
[21] 12 CFR §225.86(a)(1); 12 CFR §225.28(14)(i).
[22] 12 CFR §1016.3(r)(1).

is of the type that is available to the general public and (2) whether consumers could direct that the information not be made available to the public and the particular consumer in question has not done so. But, a consumer's lack of taking action to make their data private should not be interpreted as intending to make the data public.[23] Therefore, regulators should clarify that financial institutions are considered to have a "reasonable basis" to believe personal data has been lawfully made public if they have determined that the consumer affirmatively opted in to making their personal data publicly available.

Beyond GLBA, the CFPB should revive its withdrawn proposed rulemaking to clarify how FCRA applies to data brokers, which would have reined in data brokers' ability to sell financial and other sensitive personal data, including to AI companies.[24] The CFPB should also reinstate its final Personal Financial Data Rights Rule pursuant to Sec. 1033 of the Consumer Financial Protection Act, which would have required third parties to limit their collection, use, and retention of consumers' data to only what is reasonably necessary to provide the product or service requested by the consumer.[25] This rule also identified permissible and prohibited uses and would have required third parties to contractually commit any other third-party recipients of the data to comply with the same data minimization, accuracy, security, notification, and other requirements.[26]

Regulators should also improve privacy by prioritizing enforcement of laws against unfair or deceptive practices and civil rights laws generally. These laws help reduce privacy risks from AI because compliance requires companies to make sure their data uses are not likely to cause substantial injury to consumers, mislead consumers to their detriment, or result in discrimination.

IV. Third-party service providers and liability (Responding to Questions 19, 20, 21, and 22)

[23] Nathalie Maréchal & Nick Doty, *Meaningful Opt-Out Rights Require Companies to Do Their Part. State Governments Might Have to Make Them*, Center for Democracy & Technology (Mar. 3, 2025), https://cdt.org/insights/meaningful-opt-out-rights-require-companies-to-do-their-part-state-governments-might-have-to-make-them/.
[24] Protecting Americans From Harmful Data Broker Practices (Regulation V), 89 FR 101402, https://www.federalregister.gov/documents/2024/12/13/2024-28690/protecting-americans-from-harmful-data-broker-practices-regulation-v.
[25] 12 CFR §1033.421(a).
[26] *Id.*

Congress has many options in addressing service providers and liability. As an initial matter, Congress should not advance H.R. 4801, the Unleashing AI Innovation in Financial Services Act, or any other legislation that similarly creates a regulatory sandbox that allows financial service providers to use AI with actual consumers without complying with fair lending or consumer protection laws. Despite the at-times weak protections for financial data, Congress still should not be exempting AI systems from those protections – consumer opt-outs from sharing data is an important protection for people to have at least a modicum of control over their banking data. Given the heightened risks inherent to the financial services sector, AI uses within this area should be more carefully governed, not exempted from existing requirements through regulatory sandboxes or safe harbor provisions.

To improve monitoring of emerging risks, Congress should increase funding for the CFPB and FTC and tie that funding to increased enforcement of the Consumer Financial Protection Act and the FTC Act, respectively, with respect to AI uses in financial services. These laws prohibit practices that cause or are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers, and practices that are likely to mislead consumers acting reasonably in the circumstances to their detriment.[27] The Consumer Financial Protection Act also prohibits practices that materially interfere with a consumer's ability to understand a term or condition of a consumer financial product or service, or that take unreasonable advantage of a consumer's lack of understanding of the risks of the product or service or inability to protect their own interests in using the product or service.[28]

The limitations consumers face in understanding and controlling how AI is used in financial service and housing decisions makes enforcement of these laws especially vital. The CFPB and FTC's authorities under these statutes and their subject-matter expertise are critical to regulate companies in the financial services space that are beyond the current scope of GLBA and its implementing regulations. Therefore, Congress should ensure the CFPB and FTC are fully staffed, resourced, and directed to use funding to diligently monitor and respond to emerging risks.

[27] 12 U.S.C. §§5531(c), 5531(d); 15 U.S.C. §45(n); Federal Trade Commission, *Policy Statement on Deception* (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
[28] 12 U.S.C. §5531(d).

Congress also should pursue a strong oversight role over this industry with hearings and oversight letters examining company practices. These inquiries should include questions about changes to the companies' compliance processes pursuant to the reduction in enforcement and supervision and the changes to regulations under ECOA, the Fair Housing Act (FHA), and similar laws.

The CFPB, FTC, and Department of Housing and Urban Development have taken steps to remove provisions regarding disparate impact liability from ECOA and FHA regulations.[29] These agencies argue that the statutes do not provide for disparate impact claims. However, disparate impact liability is crucial for compliance with civil rights laws when AI is used in credit and housing decisions. AI systems may cause applicants to be denied credit or housing when the systems are trained on data that reflects a protected group's historical exclusion from these fundamental opportunities or when the systems consider factors that disproportionately affect certain protected groups. Discriminatory intent is practically impossible to prove as there is often no meaningful transparency regarding whether and how AI is used for these decisions, how the AI was trained and tested, or how it arrives at particular adverse decisions.[30] Moreover, AI systems may be created and used by multiple actors — such as the developer of an underlying model, a company that builds an application on top of the model, and a deployer of that application to make credit decisions — requiring consumers to determine the actor whose discriminatory intent is at issue.

Disparate impact liability helps hold institutions accountable by allowing people to challenge discriminatory actions that result from an AI system's flawed design or deployment, pushing financial service and housing providers to have measures in place to test AI systems and prevent discriminatory outcomes. Regulators should reverse the changes made to ECOA and FHA regulations, and Congress should ensure the underlying statutes are understood to provide for disparate impact liability.

Further, regulators should restore Supervisory Guidance SR 11-7 to reinforce expectations for financial institutions' oversight of their AI systems. SR 11-7 advises that, regardless of institutional size, capacity, and technical expertise, senior management is responsible for

[29] Consumer Financial Protection Bureau, *Final Rule on Equal Credit Opportunity Act (Regulation B),* 91 Fed. Reg. 21620 (Apr. 22, 2026); Department of Housing and Urban Development, *Proposed Rule on HUD's Implementation of the Fair Housing Act's Disparate Impact Standard*, 91 Fed. Reg. 1475 (Jan. 14, 2026).
[30] TechEquity Collaborative and Wonyoung So, *Screened Out of Housing: How AI-Powered Tenant Screening Hurts Renters* (2024), https://techequity.us/2024/07/24/screened-out-of-housing-research-paper/.

ensuring a critical analysis of their AI system's limitations, assumptions, and potential improvements takes place.[31] When those systems or capabilities are provided by third parties, financial institutions should be held responsible for assessing risks arising from those third-party relationships, engaging in due diligence in selecting third-party partners, managing contract structuring, and overseeing quality control of third-party services.

Congress should also stress the importance of staffing decisions in increasing financial institutions' ability to ensure explainability goals are met. As the Committee has learned from past hearings, small financial institutions may lack sufficient staff and resources to diagnose discrimination in their own or third-party AI systems, leaving discriminatory outcomes to go unchecked without proper channels for recourse.[32] Financial institutions with greater capacity often fail to recruit technical and policy experts who also have expertise in civil rights and bias to anticipate discriminatory impacts of AI systems and better understand what is necessary to make those systems explainable and transparent.[33]

Smaller community institutions that lack technical and policy expertise and capacity may need to be empowered to manage risk in third-party AI systems by guiding and facilitating audits. Congress should require new agency guidance specifically for smaller community institutions articulating specific factors and inquiries that community institutions should incorporate into procuring new AI and regularly reviewing the third-party AI systems they use. Congress and regulators can also explore certification or similar processes to incentivize financial institutions and third-party AI services to proactively examine their compliance.

V. Impacts on housing and workforce (Responding to Questions 32, 33, 34, 41, and 42)

AI has played an increasing role in housing and the workforce. Tenant screening companies should proactively provide landlords with detailed explanations regarding disqualifying records. Rental applicants should not be disqualified on the basis of criminal or eviction record data that

[31] Federal Reserve Board and Office of the Comptroller of the Currency, *SR Letter 11-7: Supervisory Guidance on Model Risk Management* (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf.
[32] See *Equitable Algorithms: How Human-Centered AI Can Address Systemic Racism and Racial Justice in Housing and Financial Services: Hearing before the H. Comm. on Fin. Serv. Task Force on Artificial Intelligence*, 117th Cong. (2021).
[33] Majority Staff of House Committee on Financial Services, 116th Cong., *Report on Diversity and Inclusion: Holding America's Large Banks Accountable* 43-44 (2020), https://docs.house.gov/meetings/BA/BA13/20200212/110498/HHRG-116-BA13-20200212-SD003-U1.pdf.

does not demonstrate culpability, such as an arrest record where the applicant was not convicted, or an eviction filing that did not actually result in the applicant's eviction. Tenant screening companies also should assess their products and provide landlords with documentation explaining their tenant screening methodologies and outputs, and any limitations to the detail or accuracy of their methodologies and outputs. In addition, these companies should identify alternative data that would reliably reflect a person's current ability to pay – without producing discriminatory outcomes similar to the traditional data they are supposed to substitute – and consider this data when their initial criteria would result in a denial.

Landlords should bear responsibility for understanding and proactively articulating to rental applicants the specific reasons for adverse tenant screening decisions. Landlords should not rely solely on tenant screening companies' reports to reject applicants, because these reports compile data scraped from numerous sources that may be incorrect or outdated.

Mortgage lenders and other deployers of technologies used to determine access to housing should adopt similar practices. Congress, as well as FHFA and similar agencies, should also incorporate the considerations described in Parts II and IV of these comments into legislation, regulations, and guidance for housing providers and their third-party AI vendors.

To support the workforce, developers of AI systems that are specifically intended to be used to make employment decisions, as well as the employers who use them, should be responsible for examining how their systems evaluate job applicants and employees. These examinations should include whether the attributes evaluated in workers are related to essential job functions and whether the systems are designed to accurately measure workers' skills and qualifications without disproportionately disfavoring certain protected characteristics.[34] Developers of general purpose AI systems should advise employers about the limitations of their systems in evaluating workers, and about limitations to their systems' ability to perform job functions. Employers and developers should incorporate explainability, pre- and post-deployment assessments, data minimization, and examinations of disparate impact for AI systems as described in Parts II and IV.

[34] Center for Democracy & Technology et al., *Civil Rights Standards for 21st Century Employment Selection Procedures* (2022), https://cdt.org/wp-content/uploads/2022/12/updated-2022-12-05-Civil-Rights-Standards-for-21st-Century-Employment-Selection-Procedures.pdf.

VI. Conclusion

As the Committee considers steps that Congress and regulators should take to modernize the existing body of law for AI advancements in financial services and housing, the Committee should make sure that consumer protection is not sacrificed in the name of innovation. Legislative and regulatory reforms should ensure that AI uses improve, rather than impede, access to financial services, housing, and other fundamental needs.