National Consumer Law Center

NATIONAL HEADQUARTERS
7 Winthrop Square, Boston, MA 02110
(617) 542-8010

WASHINGTON OFFICE
Spanogle Institute for Consumer Advocacy
1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
(202) 452-6252

NCLC.ORG

August 14, 2026

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Submitted online and via email to AIRFI_Data@mail.house.gov

Ranking Member Waters and members of the Committee on Financial Services:

The National Consumer Law Center, on behalf of our low-income clients, writes in response to your Request for Information regarding the application of current federal laws and regulations to the use of artificial intelligence (AI) in the financial marketplace.

In our comments below, we first highlight critical consumer protection principles that should apply to the use of AI throughout consumer financial services and products. We then provide responses to several of the Committee's enumerated questions regarding the intersection of AI and explainability standards in underwriting decisions, tenant protections, Proptech, and fair lending. (Response to Question 10 starts on page 2; Question 22 starts on page 7; Question 32 starts on page 8, and Questions 33-34 are addressed together beginning on page 11). Finally, we have attached to the end relevant prior reports, testimony, and comments that provide more detail and context for our recommendations.

Consumer Protection Principles Must Apply to AI in Financial Products and Services

Strong consumer protection laws are essential to fair and functioning markets. Artificial intelligence, and other technological developments, do not change that.

Preserve consumer protections. Fortunately, consumer protection law plainly applies regardless of whether a company uses AI. Financial institutions must continue to comply with consumer protections with every new technology they use. We urge the Committee to preserve these protections, and reject any industry asks for sandboxes, safe harbors, or preemption of state consumer protection laws. Such immunizations would encourage risky conduct, reward predatory behavior, and dangerously shift the cost of misconduct from the companies who engage in it to the people hurt by it. The Committee should also closely monitor the application of consumer protection law to agentic AI and ensure that consumers remain protected as this new technology is deployed.

Promote AI model accountability. We also urge the Committee to pay close attention to increased risks consumers may face as financial institutions and fintech companies rapidly adopt new technologies that may operate as decisionmaking "black boxes" with a veneer of objectivity and certainty that may not be validated as empirically sound or reliable.Congress must ensure that consumers–and the integrity of the financial system–are protected by meaningful safeguards, including robust enforcement of consumer protection and civil rights laws and oversight of industry to identify and remediate problems before large-scale harms occur. This should include requiring that AI models used throughout consumer financial services and products are transparent, explainable, and in compliance with fair lending and consumer protection laws, and are routinely assessed to ensure that the outputs are fair, unbiased, replicable, empirically derived and statistically sound, and accurately predict risk or other valid business objectives. As discussed in our responses to questions 10 and 22, we specifically encourage the Committee to consider strengthening the law to ensure that, across financial services and products, consumers are informed when an AI model is used for an adverse action, the specific reasons for the adverse action are explained, and consumers have a right to dispute.

Protect consumer data and consumer privacy. Increasingly vast quantities of personal information are being collected, stored, sold and used to feed AI models and decisionmaking. Consumer protection in the age of AI must pay careful attention to concerns regarding data inputs, data privacy, and data protection, as consumers face ever-increasing digital surveillance, their data is used for unforeseen purposes, and data breaches become increasingly catastrophic. Consumers should have control over their data, including the right to share or deny access to their data and a right to revoke permission and to trigger deletion of their data. Further, businesses should be limited to collect only data reasonably necessary to provide the product or service requested by the consumer, should be prohibited from using or selling the data for other purposes, and should be subject to limits on data retention and security.

Finally, we appreciate the opportunity to share our current thoughts with the Committee in response to this RFI, and we encourage the Committee to continue to seek feedback from advocates for consumers and the civil rights community as this issue continues to develop and as we monitor the application of consumer protection laws to companies using new technologies in the courts.

Responses to Selected RFI Questions

Question #10: **What kind of explainability standards should Congress and/or regulators establish to allow affected individuals to understand how any systems used by the financial services and housing industries reach their decisions, such as in underwriting decisions that may result in credit decisions?**

Hold creditors accountable for explaining adverse actions. Federal law already requires financial institutions to explain their adverse credit decisions, including any decisions made utilizing AI. For example, the Equal Credit Opportunity Act (ECOA) requires that creditors provide applicants with a statement outlining the reasons for the denial of credit or for taking other adverse action on a credit application or account.[1]

The reasons stated on the notice must be specific and indicate the principal reason or reasons for the action taken.[2] General statements, such as those that simply state that the adverse action was based on the creditor's internal standards or policies, or that the applicant failed to achieve a qualifying score on the creditor's credit scoring system, are insufficient.[3] The reasons disclosed must relate to and accurately describe those factors actually reviewed, considered, or scored.[4]

The CFPB, under guidance issued during the Biden administration and subsequently rescinded, accurately stated, "Creditors who use complex algorithms, including artificial intelligence or machine learning, in any aspect of their credit decisions must still provide a notice that discloses the specific reasons for taking an adverse action. Whether a creditor is using a sophisticated machine learning

---

[1] 15 U.S.C. § 1691(d)(2), (6).

[2] Official Interpretations of Reg. B, 12 C.F.R. pt. 1002, supp. I, § 1002.9(b)(2)-1. *See* Aikens v. Nw. Dodge, Inc., 2006 WL 59408 (N.D. Ill. Jan. 5, 2006) (ECOA does not require the creditor to utilize the exact language in the sample forms).

[3] Reg. B, 12 C.F.R. § 1002.9(b)(2).

[4] Official Interpretations of Reg. B, 12 C.F.R. § 1002.9(b) (2)-(4).

algorithm or more conventional methods to evaluate an application, the legal requirement is the same: creditors must be able to provide applicants against whom adverse action is taken with an accurate statement of reasons."[5] Additionally, "specificity is particularly important when creditors utilize complex algorithms because consumers may not anticipate that certain data gathered outside of their application or credit file and fed into an algorithmic decision-making model may be a principal reason in a credit decision, particularly if the data are not intuitively related to their finances or financial capacity."[6] The CFPB concluded that, "a creditor cannot justify noncompliance with the ECOA and Regulation B's requirements based on the mere fact that the technology it employs to evaluate applications is too complicated or opaque to understand."[7]

Explainability and transparency of creditor decisions are core to the ECOA's protections since its passage. Congress should be wary of watering down this clear cut standard, and should ensure that lenders do not simply point to opaque models or otherwise shirk ECOA requirements to provide specific and accurate explanations of the factors relied upon in making adverse decisions when using AI. Congress, regulators, and law enforcement must work together to hold industry accountable for meeting these obligations.

Require explanation of adverse actions in more contexts. While the ECOA already requires explanation of adverse actions for credit applications and accounts, the development of AI and novel decision-making models heightens the need to provide similar protections in all critical financial contexts, including rental housing decisions and bank account access. Consumers need to understand how important decisions about their lives are made, and must be provided an opportunity to identify and address errors or remediate and improve their prospects.

Currently, consumers who have had adverse actions taken against them in the rental housing and bank account contexts are supposed to receive notice of that adverse action under the Fair Credit Reporting Act (FCRA) if a consumer report was used. The adverse action notice must contain certain information, including the name, address, and telephone number of the consumer reporting agency providing the consumer report and a statement that the consumer can obtain at no charge the contents of the consumer's file from the consumer reporting agency making the consumer report if the consumer makes the request within sixty days. However, the FCRA has no requirement similar to that in the ECOA that the user provide a statement of the reasons for the adverse action or identify the items that caused the adverse action. Additionally, the consumer is only entitled to an adverse action notice under the FCRA if a consumer report prepared by a consumer reporting agency was used in making the decision.[8]

These protections are necessary but wholly insufficient. Further, even these limited requirements appear to be frequently violated. The Federal Reserve Board, which conducts consumer compliance

---

[5] Consumer Financial Protection Bureau, Consumer Financial Protection Circular 2022-03: Adverse Action notification requirements in connection with credit decisions based on complex algorithm at 3 (May 26, 2022) (rescinded), *available at* https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/. While this guidance was rescinded, it was as part of a mass withdrawal that was not based on the merits of the guidance, and the reasoning of the guidance remains valuable. *See* National Consumer Law Center, Continued Vitality of 67 Withdrawn CFPB Guidance Documents (May 13, 2025), *available at* https://library.nclc.org/article/continued-vitality-67-withdrawn-cfpb-guidance-documents.

[6] Consumer Financial Protection Bureau, Consumer Financial Protection Circular 2023-03: Adverse action notification requirements and the proper use of the CFPB's sample forms provided in Regulation B (Sept. 19, 2023) (rescinded), *available at* https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/.

[7] *Id.*

[8] 15 U.S.C. § 1681m(a).

examinations of certain state banks, listed FCRA adverse action notice violations as one of the top consumer compliance violations in 2022.[9] Consumer advocates also report that landlords often fail to provide adverse action notices when required. But many courts have interpreted the 2003 FACTA amendments to the FCRA to have eliminated consumers' ability to privately enforce the FCRA's adverse action notice requirements, leaving many consumers at a loss.[10]

We therefore encourage the Committee both to provide consumers with explanability, notice, and dispute rights whenever adverse decisions are made in significant financial and housing contexts, and to ensure the protections that currently exist under the FCRA are enforced.

Address problems associated with AI transaction monitoring tools and bank account access. In recent years, many consumers have raised concerns about bank account closures and/or freezes that seem to occur without any sudden change of behavior by the consumer or in response to a fraud dispute by the consumer (when the consumer reports unauthorized use of their account). Some consumers have also reported that even when a financial institution temporarily credits an account for a fund transfer that a consumer has disputed as unauthorized, the financial institution will then refreeze that amount or the entire account within hours after the recredit. Consumers report frustration and uncertainty tied to account closures and freezes—primarily due to the lack of information regarding why the closure or freeze occurred and the inability to access needed funds in a timely manner.

The number of consumers who have complained about checking and savings account closures to the CFPB more than doubled since 2017.[11] In 2022, the CFPB ordered Wells Fargo to pay $160 million to over one million people for improperly freezing or closing bank accounts from 2011 to 2016 when it "believed that a fraudulent deposit had been made into a consumer deposit account based largely on an automated fraud detection system."[12] Many reported stories have detailed the devastating impact sudden account closures and freezes can have on consumers, especially when they are deprived of access to

---

[9] Federal Reserve Board, Consumer Compliance Outlook (2023), *available at* https://emma-assets.s3.amazonaws.com.

[10] 15 U.S.C. § 1681m. *See* National Consumer Law Center, Fair Credit Reporting at § 9.5.5 (11th ed. 2026), *updated at* www.nclc.org/library.

[11] Consumer Financial Protection Bureau, Consumer Complaint Database, trends data for complaints received due to checking or savings account closure, https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&dateRange=All&date_received_max=2024-01-27&date_received_min=2011-12-01&has_narrative=true&issue=Closing%20an%20account%E2%80%A2Company%20closed%20your%20account&lens=Product&product=Checking%20or%20savings%20account&searchField=all&subLens=sub_product&tab=Trends. (last visited February 20, 2024). Note that the CFPB's recent announcement to stop making this data publicly available,https://www.consumerfinance.gov/about-us/newsroom/the-cfpb-to-cease-discretionary-publication-of-complaint-narratives-and-visualizations/, will significantly limit the availability of data to conduct this type of analysis going forward. https://www.nclc.org/cfpb-hides-corporate-wrongdoing-from-public-view/

[12] *In re. Wells Fargo Bank, N.A.*, CFPB No. 2022-CFPB-0011 (December 20, 2022) (consent order), *available at* https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

their funds, are not provided with any information about the reason for the institution's actions, and are not provided an opportunity to address any perceived risk.[13]
One of the reasons for the increase in account closures and freezes has to do with the increased adoption of tools utilized by financial institutions to combat payment fraud and detect suspicious activity, including adoption of AI and machine learning technologies. Fraud vigilance is critical, and new technologies can play an important role. However, these tools may harm innocent consumers if not utilized properly and if institutions do not have clear, transparent procedures and timelines in place to restore access to funds that are improperly frozen.

Financial institutions have an obligation under the Bank Secrecy Act (BSA) to ensure that they maintain and follow internal ongoing Customer Due Diligence (CDD) programs and policies. The CDD program's policies must allow the institution to understand "the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and [c]onducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information."[14]

Because of the CDD obligation and the ongoing problem of payment fraud, sometimes the appropriate response by an institution that suspects its customer is engaging in fraudulent or other illicit activity is to freeze a transaction or close an account that is being used to receive fraudulent funds before the funds are gone and more consumers can be defrauded. But sometimes financial institutions get it wrong, especially when automated tools are used. No law requires a financial institution to take these actions; it is up to the risk tolerance of the company and the internal policies set in place by the company. The only required response to potential fraud a company may need to undertake under BSA/AML law is to file a Suspicious Activity Report (SAR) if the transaction is large enough to meet the threshold reporting requirements and update their customer risk profile.[15] According to the Bank Policy Institute, "a sample of the largest banks reviewed approximately 16 million alerts, filed over 640,000 SARs, and received feedback from law enforcement on a median of 4% of those SARs. Ultimately, this means that 90-95% of the individuals that banks report on were likely innocent."[16] As these numbers demonstrate, even activity that leads to the filing of a SAR may ultimately not warrant an account freeze or closure.

---

[13] Barnard, Tara Siegel and Lieber, Ron, Banks Are Closing Customer Accounts, With Little Explanation, New York Times, (April 8, 2023), *available at* https://www.nytimes.com/2023/04/08/your-money/bank-account-suspicious-activity.html?unlocked_article_code=1.QU0.szRm.kfoZRQdD7-O6&smid=url-share; Kessler, Carson, "*A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money*," ProPublica, (July 6, 2021), available at https://www.propublica.org/article/chime; McGreevy, Patrick, "*Bank of America must provide more proof of fraud before freezing EDD accounts, court orders,*" Los Angeles Times, (June 1, 2021), *available at* https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california; KCAL News, "*Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud*," (October 29, 2020), *available at* https://www.cbsnews.com/losangeles/news/bank-of-america-freezes-edd-accounts-of-nearly-350000-unemployed-californians-for-suspected-fraud/.
[14] 31 C.F.R. § 1020.210(a)(2)(v);(b)(2)(v).
[15] Financial Crimes Enforcement Network, Customer Due Diligence Requirements for Financial Institutions, Final Rule, 81 Fed. Reg. 29398 (May 11, 2016); 31 C.F.R. 1020.210(b)(i); Office of the Comptroller of the Currency, *Bank Secrecy Act (BSA)*, *available at* https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html/.
[16] Bank Policy Institute, The Truth About Suspicious Activity Reports, (September 22, 2020), *available at* https://bpi.com/the-truth-about-suspicious-activity-reports/ (citing, Bank Pol'y Inst., *Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance*, (October 29, 2018), *available at* https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf).

To compound matters, many financial institutions believe that if an account was closed or frozen and a SAR was filed, they are not allowed to disclose the reason why the account was closed or frozen, because it would lead to the assumption that a SAR was filed. As a result, consumers are not told why their account is closed or funds are frozen, or they are given the run-around. Many consumers have reported that financial institutions reply that they cannot disclose any information as to why the account was closed or frozen. Yet financial institutions are only prohibited from disclosing the existence of the SAR, not responding to consumer concerns that their account was frozen or closed improperly.

The impact of sudden account closures in response to potential fraud on innocent consumers cannot be overstated. Often, the most vulnerable people have been denied access to their money, rendering them unable to eat or pay rent. Some impact on innocent individuals may be impossible to avoid, as banks may need to act quickly on imperfect information. But that is why it is imperative to have procedures in place to enable people to dispute account freezes and closures and get their money back as soon as possible.

If people cannot access the money they need based on red flags triggered by automated fraud tracking systems, then they need a timely solution, not another obstacle. Yet that is what occurs; consumers face obstacle upon obstacle. When a consumer complains about an account closure or freeze, the complaint is often not followed by a reasonable investigation by the financial institution that includes a discussion with the consumer or that provides any clear timeline to unfreeze their money.

NCLC has assisted many impacted consumers with complaints to the OCC, Treasury (when an impacted account was through the Direct Express program), or by leveraging connections within large financial institutions to look into an account and resolve the issue. However, this is not a sustainable solution for all impacted consumers. Policies need to change. Crude AML/CFT compliance policies and overly broad fraud responses can shut consumers out of our banking system.

Although the Electronic Fund Transfer Act (EFTA) has clear error resolution timelines and procedures when problems arise with an electronic fund transfer (EFT), problems related to checks and bank-to-bank wire transfers are often outside the scope of the EFTA.[17] When a consumer is unable to make an electronic withdrawal or transfer because of an account closure or freeze based on suspected fraud triggered by an AI or ML transaction monitoring tool, that action should be viewed as an error—an incorrect transfer of zero instead of the requested amount—triggering the error resolution rights, duties, timelines, and investigation procedures of the EFTA. The EFTA's error resolution procedures can also be triggered by the consumer's request for information about a failed EFT, which is another enumerated error under the EFTA.[18] But financial institutions and payment apps seem to believe the EFTA does not apply in this situation. Additionally, a request for information about a freeze of funds from deposited checks or a received bank-to-bank wire transfer would not be subject to the EFTA error resolution procedure, unless the consumer attempts an EFT and that transaction fails.

---

[17] Checks are outside of the scope of the EFTA. *See* 15 U.S.C. §1693a(7)(A). Although the EFTA does not directly exempt wire transfers; it exempts electronic transfers, other than ACH transfers, made "by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer." *See* 15 U.S.C. §1693a(7)(B). Regulation E and the official interpretations of Regulation E interpret that exemption to cover wire transfers using Fedwire or through a similar wire transfer system, like SWIFT, CHIPS, and Telex, that is used primarily for transfers between financial institutions or between businesses. *See* Reg. E, 12 C.F.R. § 1005.3(c)(3). As a result, banks claim that the EFTA and Regulation E protections do not apply to bank-to-bank wire transfers and these are instead covered under state law, more specifically a state's adopted version of Uniform Commercial Code Article 4A.

[18] 15 U.S.C. § 1693f(f)(6).

Question 22: What liability, if any, should be applied to financial institutions and/or third-party service providers used by financial institutions to the extent the use of AI contributes to violations of Federal law or regulation, especially where consumers are harmed? What law(s) should be amended to create this liability framework? Should there be safe harbors provided in certain circumstances? Please explain why any proposed changes may be warranted.

Consumer protection law applies regardless of technology used. Artificial intelligence does not offer a get-out-jail free card to those who use it, and financial institutions are, and must continue to be held, liable for violations of consumer protection law regardless of the type of technology they use. Existing federal consumer protection law is agnostic to underlying technologies used, and any suggestion that companies are exempt from liability to harmed consumers if the harm stemmed from use of AI or other new technology is false. The Committee should work with regulators to ensure that financial institutions using AI comply with all existing consumer protections.

Reject safe harbors and other carve-outs. The Committee should reject any calls for AI safe harbors, preemption of state laws, or other liability carve-outs that would immunize companies from accountability for violating the law or harming consumers when using AI, leaving consumers to bear the cost of companies' unfair, deceptive, discriminatory, or otherwise unlawful conduct. Adopting safe harbors would pose substantial and unwarranted risks to consumers, and transfer the cost of risk and misconduct from financial institutions who can control it to consumers who cannot. Financial institutions have been using algorithms for years without requiring legal carve-outs, and soon virtually all consumer financial products and services will use AI in some form–if they are not already. Exempting financial services companies from consumer protection liability when using AI would effectively obliterate our consumer protection laws and immunize the entire field, removing accountability for industry and turbo-charging risky practices at tremendous cost to consumers.

Nor are more limited safe harbors necessary or appropriate. While there is certainly value in encouraging industry to comply with best practices to develop, assess, and monitor AI for compliance with existing law and to meet potentially enhanced third-party or regulatory standards for AI, using exemption from consumer protection liability to incentivize such compliance is the wrong approach. Rather, the incentive should exist naturally if the standards are well-designed and thus compliance has the effect of actually reducing violations of consumer protection laws and resulting consumer harm, thereby reducing liability risk. If desired, compliance with best practices or other frameworks can be further encouraged via negative consequences for non-compliance (e.g., heightened monitoring, reputational harm, potential industry exclusion from valuable networks, etc.) rather than through assurance of immunity for compliance.

Ensure consumer protections are not disrupted by agentic AI. While it is clear that consumer protection laws apply regardless of use of AI, one area of emerging concern is how consumer protection liability will be applied by the courts when a consumer uses agentic AI in a transaction.[19] Questions include whether agentic AI tools will be recognized as agents of consumers with fiduciary duties, the consequences of their divided loyalties, who is liable when AI agents given access to a consumer's bank account or credit card make purchases or payments in excess of their intended authority, and the application of disclosure and consent protections when an AI agent rather than a consumer receives the disclosure and provides consent. We will be watching the case law in this area, and we encourage the Committee to monitor these issues as new agentic technology is deployed, to engage with the consumer

---

[19] Consumer Bankers Association, Agentic AI Payments: Navigating Consumer Protection, Innovation, and Regulatory Frameworks (Jan. 2026), *available at* https://consumerbankers.com/wp-content/uploads/2026/01/CBA-Agentic-Symposium-White-Paper-2026-01v2.pdf, at 22-31 (discussing potential risks to consumers of agentic AI in consumer payments), 36-46 (discussing application of current state and federal consumer protection law to agentic payments risks).

protection community, and to ensure that consumers are not cut out of protections as a result of agentic AI. At a minimum, consumers must have recourse under the unauthorized use, error, chargeback and dispute rights provisions in the Truth in Lending Act and the Electronic Fund Transfer Act when AI agents are involved. We urge the Committee to ensure that these important protections are not eroded and apply fully across the uses of agentic AI.

Strengthen consumer protections. As described in the answer to Question 10 above, consumers should receive adverse action notices that explain major decisions concerning access to housing and financial services, even when the decision maker did not use information in a consumer report from a consumer reporting agency. Additionally, the FCRA should at minimum be amended to clarify that FCRA's private enforcement remedy does apply to a failure to provide an adverse action notice, given that several courts have interpreted the 2003 FACTA amendments to the FCRA as eliminating consumers' ability to privately enforce the FCRA's private right of enforcement in this context

Additionally, the problem with bank account closures and freezes triggered by overly aggressive AI transaction monitoring tools could be addressed, in part, by rulemaking or guidance from the CFPB. The EFTA's error resolution procedures allow financial institutions to continue using automated fraud detection systems while ensuring that there are procedures in place for resolving disputes related to electronic fund transfers in a reasonable time and give consumers remedies when those systems get it wrong. This would ensure a consumer receives information about why their account was frozen or closed and get more timely access to their funds if the bank was in error.

More also needs to be done with respect to transactions that are not governed by the EFTA to ensure that consumers are protected against overly aggressive AI transaction monitoring tools. The most robust measure would be for Congress to act. However, the CFPB, Treasury, and bank regulators may also have authority to address some of these issues, and Congress can urge these agencies to act.

The CFPB and bank regulators can provide guidance to financial institutions about the importance of having clear procedures to enable consumers to quickly regain access to their funds when they are frozen due to concerns of suspicious activity, provide guidance as to the timeliness of returning an accountholder's funds after account closure, and specify that failing to have clear procedures and provide timely return of any funds may constitute an unfair, deceptive, or abusive business practice. Bank regulators, along with FinCEN, should provide guidance to financial institutions about what information they may and should provide to accountholders regarding freezes and account closures while still complying with the BSA. For example, they could clarify in an FAQ that, while financial institutions are not allowed to disclose that a SAR was filed, they are allowed to describe the specific activities that raised concerns, giving the consumer an opportunity to respond and appeal a decision that was made in error, or based on false assumptions or false red flags. They should also clarify that if a SAR does not lead to criminal prosecution or involvement by law enforcement for suspected money laundering/financing of terrorism activity, then a financial institution should not automatically take derisking measures and close the account based solely on the filing of a SAR, but the institution should instead take a measured, case-by-case, risk-based approach. Finally, regulators should investigate the reasons that deposit accounts are closed or frozen and the role played by AI transaction monitoring tools in those closures and freezes, and develop a strategy to minimize the number of account closures for innocent consumers.

Question #32: What tenant protections should be ensured in PropTech?

One of the most prominent uses of AI in PropTech is by tenant screening companies, as documented in the following:

- U.S. Dept of Housing and Urban Development, Office of Fair Housing and Equal Opportunity (FHEO), Guidance on Application of the Fair Housing Act to the Screening of Applicants for Rental Housing at 14-15 (Apr. 29, 2024) (withdrawn), https://web.archive.org/web/20240519122135/https://www.hud.gov/sites/dfiles/FHEO/documents/FHEO_Guidance_on_Screening_of_Applicants_for_Rental_Housing.pdf ("HUD/FHEO Tenant Screening Guidance"),

- National Consumer Law Center, Digital Denials: How Abuse, Bias, and Lack of Transparency in Tenant Screening Harm Renters at 8-9 (Sept. 2023), https://www.nclc.org/resources/digital-denials-how-abuse-bias-and-lack-of-transparency-in-tenant-screening-harm-renters

- TechEquity Collaborative, Screened Out of Housing: How AI-Powered Tenant Screening Hurts Renters, July 2024, https://techequity.us/2024/07/24/screened-out-of-housing-research-paper/

As discussed in these documents, tenant screening companies often offer products that provide a recommendation or score recommending that a landlord accept, accept with conditions, or deny rental applicants. These companies claim to use AI in producing these recommendations, but exactly how these algorithms or models work is unclear due to a lack of transparency.

Unlike credit scores, there is little empirical research about or regulatory oversight over tenant screening scores and recommendations.[20] As the CFPB noted, "common practices in financial services credit risk operations, such as documented model validation and risk management, do not appear to be prevalent in tenant risk modeling."[21] In other words, there is no reliable evidence as to whether tenant screening scores or recommendations are predictive or meaningful at all.[22]

Reliance on tenant screening scores and recommendations also disproportionately burdens tenants of color. Tenant screening companies and others may assert that relying on these automated decision-making tools helps eliminate bias.[23] However, these tools instead could worsen discrimination because bias can be introduced in multiple stages of the model development process, including through:

- reliance on data that is limited and unrepresentative, weighted or labeled in a biased way, or shaped by historical discrimination;
- bias in the design of the model or in the defining of output variables; and
- incorrect application of patterns from one situation to a different scenario.[24]

---

[20] With respect to credit scores, the implementing regulation of the federal Equal Credit Opportunity Act requires them to be "empirically derived, demonstrably and statistically sound,..." Reg. B., 12 C.F.R. § 1002.2(p)(1).
[21] CFPB, Tenant Background Checks Market at 3 (Nov. 2022), *available at* https://files.consumerfinance.gov/f/documents/cfpb_tenant-background-checks-market_report_2022-11.pdf. *Id.* at 41. ("In contrast to the documented model risk management in the financial services space, we are unaware of objective validation of tenant screening company models or detailed descriptions of the specific variables or weights used in a given model.")
[22] *Id.* at 40 ("nor is there independently validated, publicly available evidence that they reliably predict rental outcomes.")
[23] *See, e.g.*, RealPage, A Guide to Tenant Background Screening for Property Management Companies (March 19, 2026), https://www.realpage.com/blog/tenant-background-screening-guide/ ("Written criteria ensure objectivity and defend against discrimination claims.").
[24] *See* David Lehr & Paul Ohm, Playing with the Data: What Legal Scholars Should Learn About Machine Learning, 51 U.C. Davis L. Rev. 653, 662-63 (2017); Chiraag Bains, When Machines Discriminate: The Critical Role of Disparate Impact in AI Accountability at 19-24(Jan. 2026), *available at* https://civilrights.org/wp-content/uploads/2026/01/SNAPSHOT-When-Machines-Discriminate_The-Critical-Role-of-Disparate-Impact-in-AI-Accountability.pdf.

Tenant screening scores and recommendations create a misleading veneer of objectivity while concealing any underlying bias.

The HUD/FHEO Tenant Screening Guidance specifically addresses the use of artificial intelligence and machine learning in tenant screening. While it was withdrawn by the Trump Administration, the discussion by HUD staff was thoughtful and insightful, and its recommendations are worth consideration. The HUD/FHEO guidance notes that the Fair Housing Act applies broadly, including to housing decisions made using new technologies such as AI and machine learning.[25]

To address the problems posed by AI and machine learning in tenant screening, we recommend that Congress should require or urge regulators to mandate the following:

1. As recommended in the HUD guidance, tenant screening companies should be required to develop and use algorithms or models that are:

   a. more interpretable and explainable, especially when it does not meaningfully reduce accuracy or fairness;

   b. trained using demographically representative data to help ensure that the model does not erroneously learn that certain protected classes should be screened out at higher rates; and

   c. validated as having accurately and equitably predicted behaviors in the past; and periodically reassessed to ensure they continue to do so. In other words, there should be a requirement that tenant screening algorithms be empirically derived, demonstrably and statistically sound, as well as periodically re-validated, much like credit scoring models.

2. As recommended in the HUD guidance, adopt the below measures that would help improve tenant screening generally and also reduce the opacity of tenant screening algorithms and models and promote fairness in their use.

   a. Only use information relevant to whether an applicant will be a successful tenant, such as considering whether past incidents are likely to recur (e.g., eviction due to job loss); waiving screening criteria that are not relevant for an applicant's individual circumstances (e.g., minimum income requirement for an applicant whose rent will be paid by a housing voucher); prioritizing the most relevant records (e.g., most recent records versus older ones); and disregarding records without a negative outcome.

   b. Avoid the use of inaccurate data, such as using datasets that: are incomplete, missing key personal identifiers, or updated infrequently; miscategorize records; and employ matching practices that erroneously attribute records to the wrong person.

   c. Ensure transparency by: making tenant screening policies publicly available in writing; not considering records outside the scope of the policy; and providing denial letters that contain as much detail as possible as to all reasons for the denial.

   d. Provide applicants with an opportunity to dispute the accuracy or relevance of any negative information.

[25] HUD/FHEO Tenant Screening Guidance at 1 (emphasizing that the FHA "applies to housing decisions regardless of what technology is used. Both housing providers and tenant screening companies have a responsibility to avoid using these technologies in a discriminatory manner").

Questions #33 and 34 (answered together)
#33 What is specifically needed to ensure transparency and clarity in algorithms used on online real estate platforms, automated valuation models, automated underwriting systems, electronic closing products and other PropTech so that regulators and Congress can promote responsible innovation while ensuring access to fair and affordable housing and prohibiting disparate outcomes and/ or discriminatory practices?

#34: What actions should the FHFA and other similar agencies take to oversee PropTech and ensure compliance with fair lending laws and regulation?

PropTech refers to a wide range of technology and AI-driven systems used in housing and real estate related credit, many of which can result in reducing or denying access to housing. This ranges from systems that hyper-target advertising, find or manage housing, or are part of the underwriting process on real estate related transactions. Such systems may produce discriminatory output. Redfin, for example, was challenged for allegedly digitally redlining communities of color with its minimum home listing price policy that offered no marketing service for homes in certain communities.[26]

Among the many so-called PropTech tools, automated valuation models (AVMs) have come under scrutiny. Property valuation performed through an AVM[27] is based on data from traditional appraisals, public records, and private vendors.[28] Federal law requires lenders to use a state licensed or certified human appraiser,[29] but an exception to that law covers over 80% of home sales by aggregate dollar volume.[30]

Consumers depend on accurate valuations. An inaccurate AVM can overvalue or undervalue a property, creating serious, practical consequences for homeowners and buyers. Inaccurate data, for example, may lead to an appraisal waiver on an overvalued property leading a borrower to have higher LTVs than anticipated and with less equity in the property.[31]

The data fed into AVMs makes them less accurate. AVMs are trained on data that has a history of discrimination in housing and residential mortgage lending.[32] Regulators issued a final rule to address the

---

[26] National Fair Housing Alliance, Our Redfin Investigation, *available at* https://nationalfairhousing.org/issue/redfin-investigation/.
[27] The International Association of Assessing Officers defines an AVM as "A mathematically based computer software program that market analysts use to produce an estimate of market value based on market analysis of location, market conditions, and real estate characteristics from information that was previously and separately collected. The distinguishing feature of an AVM is that it is a market appraisal produced through mathematical modeling." *See* IAAO, Standard on Automated Valuation Models at 4 (July 2018), *available at* https://www.iaao.org/wp-content/uploads/Standard_on_Automated_Valuation_Models.pdf.
[28] CoreLogic, AVM FAQs (11-avm-faq-va-0804-00), https://www.corelogic.com/downloadable-docs/avm-faqs.pdf (2014).
[29] 12 U.S. Code §§ 3342, 3343.
[30] 83 Fed. Reg. 63119 (Dec. 7, 2018).
[31] *See* FHFA, Request for Information on Appraisal-Related Policies, Practices, and Processes 17-18 (Dec. 28, 2020), *available at* https://www.fhfa.gov/Media/PublicAffairs/PublicAffairsDocuments/RFI-Appraisal-Related-Policies.pdf.
[32] *See* Michael Neal, Sarah Strochak, Linna Zhu,and Caitlin Young, *How Automated Valuation Models Can Disproportionately Affect Majority-Black Neighborhoods* (Dec. 2020), *available at* https://www.urban.org/sites/default/files/publication/103429/how-automated-valuation-models-can-disproportionately-affect-majority-black-neighborhoods_1.pdf.

integrity of AVMs.[33] However, the rule does not create a private right of action. Consumers thus need regulators to supervise and enforce compliance with the rule.

While the recently passed 21st Century ROAD to Housing Act (Public Law No: 119-101) addressed some issues pertaining to appraisals, it does not affect AVMs. This is a missed opportunity that we urge regulators and Congress to redress. Our recommendations for regulating AVMs can be found on page 17 of the attached 2024 comments to the Treasury Department[34] and in our August 2023 Comments to Federal Regulators on Quality Control Standards for AVMs.[35]

With respect to PropTech, all agencies should ensure that hyper-targeted online marketing of financial products does not lead to steering and digital redlining. Under the Biden Administration, the U.S. Department of Housing and Urban Development (HUD) issued guidance on advertisement of housing and credit for real-estate related transactions.[36] The agency noted that technology can be used to target advertising toward some consumers and away from others. Whether done deliberately or through the operation of complex automated systems, such ad-delivery systems have the potential to cut certain consumers off from important housing and credit opportunities.[37] This occurs when targeted ads deny consumers information about housing opportunities, target vulnerable consumers for predatory products or services, discourage or deter potential consumers, advertise different prices or conditions to consumers, steer home-seekers to particular neighborhoods, or charge advertisers higher amounts to show ads to some consumers.[38] Such discriminatory advertising practices may violate the Fair Housing Act when aimed at protected classes and should be closely scrutinized and regulated.

Federal agencies overseeing the use of this technology should take common-sense actions to protect consumers. First, federal agencies should model the transparency they want to see in the private market with respect to the use of AI. This includes disclosing information related to any use of AI as part of the development of rulemaking or guidance documents.

Second, federal agencies should ensure compliance with fair lending, civil rights and consumer protection laws in rulemaking and guidance related to AI systems. This should include a focus on transparency and explainability. Further, federal agencies should:

- Examine financial institutions' use of AI models in housing and credit decisions and develop guidance and other information on the use of this technology. This includes updating model risk management guidance;

- Designate AI as a systemic risk to consumers in all guidance issued to financial institutions;

---

[33] *See* CFPB Press Release, *Agencies Issue Final Rule to Help Ensure Credibility and Integrity of Automated Valuation Models* (July 17, 2024).
[34] National Consumer Law Center, Comments to the U.S. Dep't of Treasury re: Request for Information on Uses, Opportunities, and Risks of Artificial intelligence in the Financial Services Sector (Aug. 12, 2024).
[35] National Consumer Law Center and National Fair Housing Alliance, Comments to the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, FDIC, Nat'l Credit Union Administration, CFPB, and FHFA re: Quality Control Standards for Automated Valuation Models (Aug. 21, 2023).
[36] U.S. Department of Housing and Urban Development, *Guidance on Application of the Fair Housing Act to Advertising of Housing, Credit, and Other Real Estate-Related Transactions through Digital Platforms* (April 29, 2024) (withdrawn), *available at* https://web.archive.org/web/20240519122135/https://www.hud.gov/sites/dfiles/FHEO/documents/FHEO_Guidance_on_Screening_of_Applicants_for_Rental_Housing.pdf.
[37] *See id.*
[38] *See id.* at 2.

- Require that financial institutions routinely test their models to ensure the outputs are fair, empirically derived, and statistically sound, and accurately predict risk or achieve other valid objectives;
- Ensure that financial institutions produce models that are explainable and in compliance with fair lending and consumer protection laws;
- Use supervisory and enforcement authority to prevent and address harm from financial institutions' use of AI models;
- Conduct research regarding the use of AI in credit, banking and other consumer-facing activities, especially the effect on consumers of color and other protected classes;
- Hire individuals from diverse backgrounds to evaluate the effect of AI on consumers of color and other protected groups; and
- Engage a diverse group of key stakeholders, including civil rights organizations, consumer advocates, and impacted community members to receive ongoing feedback on regulatory actions.

Finally, we note that the current administration, through Executive Orders, regulations, guidance, and by lack of enforcement, supervision, and oversight of companies, has aggressively sought to curtail disparate impact liability for violations of fair lending and civil rights laws. We urge Congress to protect and preserve disparate impact liability to protect consumers from being unfairly and unnecessarily excluded from economic opportunities. This is particularly important in the context of AI: requiring that consumers prove that a financial services company that used AI, or that the developer of that AI, intentionally discriminated through its AI system would create an unreasonable bar for proving discrimination and would dramatically reduce pressure on companies to ensure that the systems they rely on are fair to all.

***

Thank you for your consideration of these comments. Please reach out to Abby Shafroth, Chi Chi Wu, Odette Williamson, and Carla Sanchez-Adams at the National Consumer Law Center if you wish to discuss any of this information further.

Sincerely,

Abby Shafroth
Managing Director of Advocacy
National Consumer Law Center

Attachments

A. National Consumer Law Center, Comments to the U.S. Dep't of Treasury re: Request for Information on Uses, Opportunities, and Risks of Artificial intelligence in the Financial Services Sector (Aug. 12, 2024)

B. National Consumer Law Center and National Fair Housing Alliance, Comments to the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, FDIC, Nat'l Credit Union Administration, CFPB, and FHFA re: Quality Control Standards for Automated Valuation Models (Aug. 21, 2023)

C. National Consumer Law Center, Digital Denials: How Abuse, Bias, and Lack of Transparency in Tenant Screening Harm Renters (Sept. 2023)

D. National Consumer Law Center, Comments to the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System (Board), and FDIC re: Request for Information on Potential Actions to Address Payments Fraud (Sept. 18, 2025) (including discussion of impact on low-income consumers and potential responses to over-aggressive or erroneous algorithmic fraud detection at pp.14-17)

E. National Consumer Law Center, Testimony of Carla Sanchez-Adams, National Consumer Law Center, “Fraud in Focus: Exposing Financial Threats to American Families”: Oversight and Investigations Subcommittee of the U.S. House Financial Services Committee (Sept. 18, 2025) (including discussion of impact on low-income consumers and potential responses to over-aggressive or erroneous algorithmic fraud detection at pp.37-40)

F. Consumer Bankers Association, Agentic AI Payments: Navigating Consumer Protection, Innovation, and Regulatory Frameworks (Jan. 2026) at 22-31 (discussing potential risks to consumers of agentic AI in consumer payments), 36-46 (discussing application of current state and federal consumer protection law to agentic payments risks); 48-51 (discussing potential solutions, including adoption of an FCRA-like dispute system beyond the credit reporting context and RESPA-style prohibitions on kickbacks and self-dealing)