September 22, 2020

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, DC 20429
comments@fdic.gov

RE: Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services [Docket ID 2020-16058; RIN 3064-ZA18; 85 FR 44890]

Dear Secretary Feldman:

The Americans for Financial Reform Education Fund (AFR Education Fund) and Demand Progress Education Fund (DPEF) appreciate the opportunity to comment on the above Request for Information (RFI) by the Federal Deposit Insurance Corporation (FDIC). AFR Education Fund is a coalition of more than 200 national, state, and local groups who have come together to advocate for reform of the financial industry. Members of AFR Education Fund include consumer, civil rights, investor, retiree, community, labor, faith based, and business groups. DPEF is a fiscally-sponsored project of New Venture Fund, a 501(c)3 organization. DPEF and our more than two million affiliated activists seek to protect the democratic character of the internet — and wield it to make government accountable and contest concentrated corporate power.

We write to express our concerns with the recent Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services (RFI).[1] As the Federal Deposit Insurance Corporation (FDIC) reassesses third-party partnerships regarding financial technology (fintech), we urge it to refrain from delegating its responsibilities to a public-private standard-setting organization (SSO) and instead

[1] FDIC, Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services, RIN 3064–ZA18, 85 FR 44890 (July 20, 2020), https://www.fdic.gov/news/press-releases/2020/pr20083a.pdf [hereinafter RFI].

to develop its own expertise in the context of a robust, precautionary, approach to oversight. Facilitating compliance with SSO standards is not an acceptable means of regulation, nor an acceptable alternative to regulation. To the extent collaboration with an SSO is required, we encourage the FDIC to collaborate with existing public bodies, such as the National Institute for Standards and Technology (NIST). We especially oppose privatizing responsibility for standard-setting at a time when the FDIC and other regulators are opening the banking franchise to Big Tech and surveillance-driven technology.[2]

Banks are increasingly partnering with a wide range of third-party non-bank "fintechs" — "a label so broad as to be meaningless."[3] Some of these business partnerships may provide important benefits to individual customers. But others exist primarily as a means for the nonbank company to borrow a bank charter in order to evade state consumer protection laws.[4] High-cost "rent-a-bank schemes" in particular, tend to hide behind these deals.

The answer to this problem is not to provide more flexibility for insured depository institutions (IDIs) to engage in novel partnerships using technology banking regulators have not sufficiently studied. Nor is it to allow fintech or tech firms more direct involvement in the banking system, as the FDIC plans to do with its Industrial Loan Charters (ILCs)[5] and the Office of the Comptroller of the Currency (OCC) via the provision of a Special Purpose National Bank Charter and Payments Charter.[6] It is to protect the integrity of the banking and broader financial system.

The federal government has also created its own instrumentalities for developing technological standards. Most importantly, NIST, a part of the U.S. Department of Commerce, was established in 1905 to promote competitiveness: it establishes standards with respect to innovations as diverse as advanced nanomaterials, computer chips, and (most relevantly) information technology.[7] It is remarkable that although the RFI claims the FDIC envisions "a

---

[2] *See, e.g,* Lev Menand & Morgan Ricks, *Policy Spotlight Lacewell v. OCC,* JUST MONEY (Aug. 5, 2020), https://justmoney.org/lacewell-v-occ/ (discussing the OCC's plans to grant new "special purpose" national bank charters to fintech companies that do not issue or maintain deposit balances, exempting them from key federal regulations).

[3] Letter from Nat'l Consumer Law Ctr. to OCC 6 (Aug. 3, 2020), https://www.nclc.org/images/pdf/rulemaking/2020-OCC-fintech-NCLC-comments.pdf.

[4] *Id.* at 6-7.

[5] *See*, *e.g.,* Letter from AFR Education Fund & DPEF to FDIC (July 2, 2020), https://ourfinancialsecurity.org/2020/07/joint-letter-afr-ed-fund-and-demand-progress-ed-fund-send-letter-to-fdic-on-unacceptable-ilc-rule/.

[6] *See*, *e.g.,* Letter from Ams. for Fin. Reform to FDIC (Jan. 17, 2017), https://ourfinancialsecurity.org/2017/01/letter-regulators-afr-comment-special-purpose-national-bank-charters-fintech-companies/; Letter from Nat'l Consumer Law Ctr. to OCC (Aug. 3, 2020), https://www.nclc.org/images/pdf/rulemaking/2020-OCC-fintech-NCLC-comments.pdf.

[7] *About NIST*, NIST, https://www.nist.gov/about-nist (last visited Sept. 22, 2020).

collaboration among an SSO, the FDIC, and other stakeholders to set standards under an SSO," it does not explicitly identify NIST as a stakeholder.[8] NIST already coordinates agency interaction with private standards bodies per federal law.[9] The agency has established standards concerning artificial intelligence and algorithmic accountability, as well as multiple facets of data privacy, security, and efficacy, even establishing guidelines for the use of blockchain technology.[10] Federal agencies already use a common framework developed by NIST to manage their own cyber risk.[11] Indeed, the FDIC is already working with NIST regarding internal data breaches.[12]

Moreover, while the RFI also points toward a "voluntary conformity assessment process through accredited, independent certification organizations", the FDIC does not follow the 2013 OCC Guidance in encouraging banks to seek certifications of certain technologies by NIST.[13]

We urge the FDIC to refrain from establishing an industry-led or industry-driven SSO. According to the OCC Guidance on third-party relationships, a bank's effective risk management process must include proper due diligence in the mere selection of a third party.[14] With influence over entry and exit into the fintech sector, an industry-led SSO is likely to usurp authority that properly belongs with the regulators of IDIs (not to mention antitrust authorities).

While privatized standard-setting bodies may certainly assist in the management of dynamic, complex systems, they should also be approached with prudence. The considerations and judgments produced by SSOs are not always easily understood by the public or regulators, and thus raise the possibility of ineffective reform.[15] In rapidly changing fields, like the fintech sector, developing a set of "best practices" may provide very little insight to the public.[16]

---

[8] RFI at 10.

[9] *See, e.g.,* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 191 (2019).

[10] NIST releases Version 1.0 of its Privacy Framework, 2020 WL 416328 ("Like all NIST standards, the Privacy Framework is a voluntary tool intended to help organizations manage privacy risks arising from products and services, and to demonstrate compliance with laws affecting them such as the California Consumer Privacy Act or the European Union's General Data Protection Regulation.")

[11] *See* Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017.

[12] *See* House Science panel blasts FDIC for failing to report another data breach, 2016 WL 6246205.

[13] ¶ 35-522 GUIDANCE ON MANAGING RISKS FROM THIRD-PARTY RELATIONSHIPS, Fed. Bank. L. Rep. P 35-522.

[14] *Id.*

[15] *See* COHEN, *supra* note 9, at 191.

[16] *See*, *e.g.*, Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U.L. REV. 773, 776–77 (2020), (...compliance professionals often frame the law in accordance with managerial values like operational efficiency and reducing corporate risk rather than the substantive goals the law is meant to achieve, like consumer protection or equality. This opens the door for companies to create structures, policies, and protocols that comply with the law in name only. As these symbolic structures become more common, judges and policymakers defer to them as

Moreover, these types of organizations often deploy trade secrets law to shield their decisions from scrutiny as a matter of course.[17]

In general, the risks of delegation outweigh the rewards. We already have two empirical examples of how highly professionalized standard-setting can lead to catastrophic consequences in the financial sector. First, the integrity of the professional consensus on so-called "generally accepted accounting principles" (GAAP) collapsed in light of the Enron scandal.[18] Secondly, the capital adequacy and creditworthiness assessments of credit rating agencies (CRAs) arguably facilitated the Global Financial Crisis.[19] Historically, public interest groups have been excluded from industry-led standard-setting spaces, and are forced to rely on black-box testing and anecdotes to try to understand technologies, including their potentially discriminatory impact.[20] With no watchdogs in place, an industry-led SSO is likely to develop methodologies based on certain assumptions about the cost and benefits of a technology for partnering companies, but they will not necessarily pay close attention to the potential impacts on users.[21]

In general, we echo our previous calls for regulators to adopt a precautionary approach to digital banking activities. We should refrain from assuming these activities are significantly different to those covered by existing regulations. At the same time, we should bear in mind that certain technologies should have no place in our financial system whatsoever.[22]

The FDIC Should Not Irresponsibly Delegate Core Regulatory Functions

We consider the FDIC's third party service provider management and supervision duties

---

paradigms of best practices or as evidence for an affirmative defense or safe harbor, mistaking mere symbols of compliance with adherence to legal mandates.")

[17] *See* COHEN, *supra* note 9, at 191.

[18] *See*, *e.g.,* William W. Bratton, *Enron and the Dark Side of Shareholder Value*, 76 TUL. L. REV. 1275, 1354 (2002) (arguing "standards only work when the actor authorized to apply them is ready to take responsibility for a judgment call); William K. Black, *The Department of Justice "Chases Mice While Lions Roam the Campsite": Why the Department Has Failed to Prosecute the Elite Frauds That Drove the Financial Crisis*, 80 UMKC L. REV. 987, 1005 (2012) (arguing problems with GAAP persisted from the Enron scandal to the GFC).

[19] *See*, *e.g.,* Sid Verma, *The Great Escape: How Credit Raters Ducked Reform,* BLOOMBERG (Aug. 2, 2017), https://www.bloomberg.com/news/articles/2017-08-02/the-great-escape-how-the-big-three-credit-raters-ducked-reform.

[20] COHEN, *supra* note 9, at 193.

[21] *Id.* at 194.

[22] *See*, *e.g.,* Letter from AFR Education Fund, DPEF, et al. to OCC (Aug. 3, 2020), https://ourfinancialsecurity.org/2020/08/letter-to-regulator-occ-should-adopt-precautionary-approach-to-digital-banking-activities/.

to be core functions of the FDIC. It is incumbent on the FDIC to examine and properly supervise the relationships of depository institutions under its regulatory purview.[23] The FDIC reviews a financial institution's management of significant third-party relationships in the context of the normal supervisory process.[24] When circumstances warrant, the FDIC may use its authority to examine the functions or operations performed by a third party on the IDI's behalf. This review pertains to safety and soundness, consumer protection, and civil rights laws: all critical dimensions of financial services. Banking regulators may also take enforcement actions against "institution-affiliated parties" that have engaged in knowing or reckless conduct that "caused or is likely to cause more than a minimal financial loss to, or a significant adverse effect on, the insured depository institution."[25]

The FDIC also has responsibility to assess the third party's information security program. Generally, a third-party contract must already include provisions for periodic independent internal or external audits of the third party, and relevant subcontractors.[26] But responsibility ultimately resides with FDIC to determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. For example, like all banking regulators, the FDIC is charged with supervising the supply of third-party payment services for operational risk.[27] At a time when most people in the United States are using mobile financial services to pay bills, this security function is indispensable to the general workings of the economy. IDIs have been held responsible for the sales practices of third parties that have marketed products on their behalf.[28] It would be difficult for the FDIC to properly regulate this space without direct oversight.

---

[23] *See*, *e.g.,* FFIEC, Risk Management of Outsourced Technology Services, n.2 (Nov. 28, 2000), https://www.ffiec.gov/PDF/pr112800_guidance.pdf.

[24] RFI at 5; 12 U.S.C. §§ 1464(d)(7), 1867(c)(1); 12 U.S.C. § 1867(c)(1) ("whenever a depository institution that is regularly examined by an appropriate Federal banking agency . . . causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises . . . such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the depository institution itself on its own premises."); *see also* 12 U.S.C. § 1464 (d)(7).

[25] Matthew W. Swinehart, *Modeling Payments Regulations and Financial Change,* 67 U. KAN. L. REV. 83, 113 (2018).

[26] *See* ¶ 35-522 GUIDANCE ON MANAGING RISKS FROM THIRD-PARTY RELATIONSHIPS, Fed. Bank. L. Rep. P 35-522.

[27] *See, e.g.,* Swinehart, *supra* note 25, at 112.

[28] *See, e.g.,* Press Release, CFPB, CFPB Orders Santander Bank to Pay $10 Million Fine for Illegal Overdraft Practices (Jul. 14, 2016), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-orders-santander-bank-pay-10-million-fine-illegal-overdraft-practices/; Press Release, CFPB, CFPB Orders American Express to Pay $59.5 Million for Illegal Credit Card Practices (Dec. 23, 2013), https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-american-express-to-pay-59-5-million-for-illegal-credit-card-practices/; Press Release, CFPB, CFPB Orders Chase and JPMorgan Chase to Pay $309 Million Refund for Illegal Credit Card Practices (Sept. 19, 2013), https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-chase-and-jpmorgan-chase-to-pay-309-million-refund-for-illegal-credit-card-practices/.

If it is the case that FDIC personnel lack the expertise or resources to properly assess new technologies, outsourcing that responsibility will only entrench the problem. In the context of internet-based governance, legal language is often produced by computer scientists and engineers, and unfamiliar to many regulators and policymakers.[29] If banking continually moves toward the use of new models, would the FDIC simply retreat further from its legislative mandate?

Although the RFI suggests that the FDIC "is not considering substantive revisions to its existing supervisory guidance", this is misleading and unrealistic.[30] History has shown that the politics of multi-stakeholder standardization diminishes our ability to disentangle technical commitments from substantive policy commitments.[31] Concerns about fundamental rights tend to disappear in a cascade of jargon.[32] Alleged methodological and technical concerns should remain under the public eye, lest they involve or create substantive public interest issues that would otherwise be obscured.

It is also worth considering that technologies that outstrip the ability of regulators to regulate them should simply be prohibited. The FDIC cannot ensure that an industry-led SSO would abide by a public interest mandate. Strikingly, it appears the FDIC would not have supervisory authority over the SSO. It is troublingly unclear how an SSO would be regulated or if the FDIC would even be able to revisit an SSO's decisions. This raises the possibility that the SSO would sanction irresponsible activity or industry would use the SSO to avoid basic responsibilities. We are concerned that an industry-led SSO would become a liability shield for companies the FDIC is responsible for regulating.

For instance, as Professor Chris Odinet argues in his comment letter concerning the RFI's relevance to the Fair Housing Act (FHA), HUD's final rule states that the defendant can show that the challenged policy or practice advances a valid interest or legitimate objective, which includes practical business, profit, and policy considerations.[33] An IDI, a fintech firm, or an IDI partnering with a fintech firm to use its alternative credit scoring model may be able to provide such a justification easily by indicating it is part of their practical business plan to obtain approval from a SSO.[34] Such an approach makes it all too easy for the defendant to avoid scrutiny and creates more hurdles for the victim of discrimination.

---

[29] COHEN, *supra* note 9, at 232-233.
[30] RFI at 7.
[31] *See* COHEN, *supra* note 9, at 233.
[32] *Id.*
[33] *See* Letter from Prof. Christopher K. Odinet, Prof. of Law, Iowa Univ. L. Sch. to FDIC (Sept. 22, 2020), https://www.fdic.gov/regulations/laws/federal/2020/2020-request-for-info-standard-setting-3064-za18-c-009.pdf.
[34] *Id.*

Similar problematic dynamics may attend AML transaction monitoring models, customer service models, business development models, fraud models, etc. We have enumerated just a few consumer protection concerns in this comment.

Privatization and Independent Certification Would Likely Favor Incumbents and Lead to Corruption

We are also concerned that certain IDIs or other actors would capture or commandeer an industry-led SSO to offload responsibility for assessing the risk of their own models or those of fintech partners.

DPEF's experience with SSOs in the technology space has not given us any cause for comfort. For instance, the Internet Corporation for Assigned Names and Numbers (ICANN), the not-for-profit body that oversees the Internet's domain name system, was established by the U.S. Department of Commerce in 1998.[35] In 2006, the Department lost residual authority over this body and it was privatized entirely.[36] Recently, ICANN attempted to sell the .ORG domain registry (crucial digital infrastructure) to private equity firm Ethos Capital. They were only prevented from doing so by a large consortium of nonprofits and civil liberties organizations — including DPEF and AFR Education Fund — that understandably feared a profit-minded multi stakeholder group would raise registration fees, censor members, and collect and monetize web browsing data.[37]

There is no reason to imagine an industry-led voluntary certification program would improve competition for small IDIs like community banks or even for fintech start-ups. Some representatives of smaller IDIs have expressed concerns that the costs associated with the financial institutions' review of both models and third-party providers of models can create barriers to entry.[38] However, we are more concerned that incumbent institutions — especially those with prior experience influencing multistakeholder technological platforms — would exercise disproportionate control over the SSO. Even at the international level, many SSOs have

[35] ICANN has been formally organized as a nonprofit corporation "for charitable and public purposes" under the California Nonprofit Public Benefit Corporation Law. Prior to the establishment of ICANN, the internet's core address and routing functions were managed via contracts with the U.S. Department of Defense. *ICANN History*, ICANN, https://www.icann.org/history (last visited Sept. 22, 2020).
[36] Press Release, National Telecommunications and Information Administration (NTIA), NTIA Finds IANA Stewardship Transition Proposal Meets Criteria to Complete Privatization (June 9, 2016), https://www.ntia.doc.gov/press-release/2016/iana-stewardship-transition-proposal-meets-criteria-complete-privatization.
[37] *See, e.g.*, Karen Gullo & Mitch Stoltz, *Victory! ICANN Rejects .ORG Sale to Private Equity Firm Ethos*, ELECTRONIC FRONTIER FOUND. (Apr. 30, 2020), https://www.eff.org/deeplinks/2020/04/victory-icann-rejects-org-sale-private-equity-firm-ethos-capital.
[38] RFI at 5.

purported to support competition, but ultimately result in rent-seeking by larger firms with better funding and better connections to technologists.[39]

In general, reliance on algorithm-based performance standards has previously led to a gamification dynamic — large and powerful firms have incentives to pass the test, but not necessarily adhere to the spirit of its purpose.[40] By contrast, we expect smaller IDIs to feel constrained to enter into relationships for the provision of models or services with only those fintechs that are certified by the SSO, which would most likely be well-established firms, including those tethered to Big Tech titans like Amazon, Apple, Google, and Facebook.[41]

Finally, the use of a fee-based voluntary certification program risks creating a two-tiered system for conducting due diligence and ongoing monitoring of third-party providers. In one tier, IDIS with significant influence may be able to purchase a "rubber stamp." In the other tier, IDIs working with non-certified third parties would remain subject to more intense, direct scrutiny by the FDIC. In this scenario, allowing safe harbors for larger and influential firms would likely undermine trust in new technologies and could also discourage innovation.

New Digital Banking Activities Raise Consumer Protection Risks, Threaten Our Civil Rights, and Can Lead to Disparate Impact

The RFI asks if there are currently factors that inhibit the adoption of technological innovations.[42] It does not question whether the ostensibly relevant innovations are appropriate for IDIs or their customers. Treating innovation and liberalization as unqualified goods leads regulators to ignore both considerations of equity and long-term innovation.[43] Nascent technological innovations tend to make it more difficult for individual consumers, groups of consumers, or public interest organizations to see if and how different users of a technology may be treated differently, or there may be a discriminatory impact. This makes it that much more

---

[39] COHEN, *supra* note 9, at 206.
[40] *See, e.g.,* Cary Coglianese & Jennifer Nash, *The Law of the Test: Performance-Based Regulation and Diesel Emissions Control*, 34 YALE J. ON REG. 33-90 (2017).
[41] The expanding presence of these companies in this space cannot be overstated. For example, on August 23, 2019, Rep. Nydia Velázquez (D-NY) and Rep. Katie Porter (D-CA) sent a letter to FSOC asking that Amazon Web Services, Microsoft Azure, and Google Cloud be considered "systemically important financial market utilities." Pete Schroeder, *U.S. House lawmakers ask regulators to scrutinize bank cloud providers*, REUTERS (Aug. 23, 2019), https://www.reuters.com/article/us-usa-congress-cloud/u-s-house-lawmakers-ask-regulators-to-scrutinize-bank-cloud-providers-idUSKCN1VD0Y4. *See also*, John Detrixhe, *Amazon is invading finance without really trying*, QUARTZ (Nov. 1, 2017), https://qz.com/1116277/amazons-aws-cloud-business-is-reshaping-how-the-financial-services-industry-works/; Brendan Pedersen, *As states and OCC keep butting heads, does innovation suffer?*, AM. BANKER (Sept. 01, 2020), https://www.americanbanker.com/news/as-states-and-occ-keep-butting-heads-does-innovation-suffer.
[42] RFI at 11.
[43] COHEN, *supra* note 9, at 233.

important that regulators have and use visibility into processes and outcomes, and that they provide maximum possible transparency for the public. If the FDIC lacks the technical know-how to regulate properly, it is only cementing a paradox: effective control of data-intensive processes requires technological know-how, but the very process of optimizing controls in this way only makes governance more opaque and less accessible to the broader public.[44]

In general, the FDIC should be more mindful of consumer protection risks presented by third-party models or technologies, to ensure they are developed and operated in compliance with applicable consumer protection laws and regulations, which may include, for example, fair lending laws, privacy laws, and prohibitions against unfair, deceptive, or abusive acts or practices.[45] As IDIs increasingly enter into partnerships with technology companies and adopt new tools themselves, we maintain deep concerns regarding their use of artificial intelligence and predictive analytics for marketing, loan underwriting and monitoring, and the pricing of products and services. Data analytics can potentially benefit individual consumers, especially consumers who have a "thin file" or no file on record with a traditional credit reporting agency.[46] However, use of data analytics can also worsen existing disparities.[47] In light of the way that exploitation of unbanked and underbanked communities of color is baked into our financial system, industry plans for greater "financial inclusion" demand careful scrutiny.[48]

---

[44] *Id.* at 234.

[45] *See, e.g.,* Equal Credit Opportunity Act, 15 U.S.C. 1691-1691f; Fair Credit Reporting Act, 15 U.S.C. 1681-1681x; Interagency Statement on the Use of Alternative Data in Credit Underwriting, FIL-82-2019 (Dec. 13, 2019); Interagency Fair Lending Examination Procedures (Aug. 2009); Policy Statement on Discrimination in Lending, FR Doc. No. 94-9214 (Apr. 15, 1994); Dodd-Frank Act, Title X, Subtitle C, Sec. 1036; Pub. L. 111-203 (July 21, 2010).

[46] National Bureau of Economic Research, The Role of Technology in Mortgage Lending, Working Paper 24500, April 2018 *available at* https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr836.pdf.

[47] *See, e.g.*, Carol Evans, Board of Governors of the Federal Reserve System, *Keeping Fintech Fair: Thinking about Fair Lending and UDAP Risks*, Consumer Compliance Outlook (Second Issue 2017) 4 ("[T]he fact that an algorithm is data driven does not ensure that it is fair or objective."); *Banking on Your Data: The Role of Big Data in Financial Services: Hearing Before the H. Comm. on Fin. Services*, 116th Cong. 20-21 (2019) (Statement of Lauren Saunders, Assoc. Dir., Nat'l Consumer Law Center), *available at* https://www.nclc.org/images/pdf/cons-protection/testimony-lauren-saunders-data-aggregator-nov2019.pdf (discussing fintech and the Equal Credit Opportunity Act); *Banking on Your Data: The Role of Big Data in Financial Services: Hearing Before the H. Comm. on Fin. Services*, 116th Cong. 20-21 (2019) (Statement of Dr. Seny Kamara, Assoc. Prof., Dept. of Comp. Sci., Brown Univ.), *available at* https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-kamaras-20191121.pdf ("[Algorithmic bias] is a serious concern in the context of the Equal Credit Opportunity Act and the Fair Housing Act, both of which prohibit discriminatory lending practices").

[48] *See, e.g,* Nat'l Consumer Law Ctr., Past Imperfect: How Credit Scores and Other Analytics "Bake In" and Perpetuate Past Discrimination 2, (2016), http://www.nclc.org/images/pdf/credit_discrimination/Past_Imperfect050616.pdf [https://perma.cc/S8ED-WTDR].

Today, the use of data impacts the marketing, pricing, delivery, and implementation of almost every product, including financial services products.[49] It brings both advantages and disadvantages. So-called "alternative data" can be used inappropriately to charge higher prices to those least able to afford them. Analysis of price sensitivity and propensity to comparison shop may lead to higher prices for less sophisticated consumers, those with more limited internet access, those with fewer banks in their community, and those with fewer options.

IDIs and fintech partners are increasingly using IDI transaction data to evaluate credit applications.[50] Banks may access data in their own customers' accounts, or they may use services such as Experian Boost (using utility and telecommunications payments as identified in bank account records) and UltraFICO (using bank account transactions). Banks also partner with lenders that access transaction data through data aggregators.[51] Banks also increasingly monitor non-bank payments.

This trend raises myriad concerns. Analysis of the patterns of deposits into an account could lead to lending based on ability to collect, not ability to repay. Among other problems, this would likely lead to discrimination against recipients of government assistance, including elderly and disabled consumers. Data that goes into lending or other decisions could be attributed to the wrong consumer or be otherwise erroneous. The conclusions of computer algorithms could be off-base. The Fair Credit Reporting Act (FCRA) is aimed at ensuring accuracy, predictiveness, transparency, and appropriate use of information that is used to make decisions about people. Those purposes apply equally to decisions made through analysis of alternative data — shifting oversight to an industry-led body simply because the technology is difficult to understand would be inappropriate.

As even industry commentators have noted, certification cannot control how an IDI's data — and thus consumer data — would be used.[52] This would leave little recourse for consumers, including victims of discrimination. Too often, promises of technological empowerment yield

---

[49] *Rent-A-Bank Schemes and New Debt Traps: Assessing Efforts to Evade State Consumer Protections and Interest Rate Caps*, 116th Cong. 20-21 (2020) (Statement of Lauren Saunders, Assoc. Dir., Nat'l Consumer Law Center), *available at* https://financialservices.house.gov/uploadedfiles/lauren_saunders_testimony_on_rent_a_bank_hearing_revised_2-5-20.pdf.

[50] Account data will almost certainly exhibit disparities by race because one of the factors used by scoring models is likely to be overdrafts. African-Americans are disproportionately affected by bank overdraft practices, 25 which often encourage people to overdraft rather than helping them avoid fees. NCLC Letter, *supra* note 4, at 11, https://www.nclc.org/images/pdf/rulemaking/2020-OCC-fintech-NCLC-comments.pdf.

[51] Some financial services companies have argued that the security practices of data aggregators are not comparable to the standards applied at banks and the security practices of consumer fintech application providers are even weaker. American Bankers Association, *Fintech – Promoting Responsible Innovation* (May 2018), at 3-4, *available at* https://www.aba.com/Advocacy/Documents/fintech-treasury-report.pdf.

[52] Letter from Abrigo to FDIC (Sept. 22, 2020), https://www.fdic.gov/regulations/laws/federal/2020/2020-request-for-info-standard-setting-3064-za18-c-002.pdf.

"predatory inclusion" — a process whereby financial institutions offer needed services to specific classes of users, but on exploitative terms that limit or eliminate their long-term benefits.[53] In general, many longer-term loans originated based on alternative data are marketed toward "underbanked" low and moderate income families, but carry extremely high interest rates and are made with little regard for the borrower's ability to repay the loan while meeting other expenses.

Creditworthiness is often determined by a closed box of algorithms that assesses our 'digital character' in an opaque manner.[54] Firms using algorithmic technologies may analyze this data and make decisions in a manner that perpetuates discrimination.[55] In theory, facially neutral algorithms mitigate the risk that consumers will face intentional discriminatory treatment based on protected traits such as race, gender, or religion.[56] But evidence demonstrates that the data sets being used are often incomplete or inaccurate, and that discriminatory outcomes can result from use of data that correlates with race.

Creditors using alternative data may run afoul of credit discrimination laws if use of that data leads to disparate outcomes. The Equal Credit Opportunity Act (ECOA) prohibits credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, and other factors.[57] The FHA prohibits discrimination in the sale, rental or financing of dwellings and other housing-related activities on the basis of race, color, religion, national origin, sex, disability or familial status.[58] Both statutes prohibit policies or practices that have a disproportionately negative impact on a protected class even though the creditor has no intent to discriminate and the practice appears neutral on its face.

Much like the factors that drive the disparities in traditional credit scores, the new sources of data reflect deeply ingrained structural inequalities in employment, education, housing and economic opportunity.[59] Geolocation data reflects deeply entrenched racial and ethnic

---

[53] Louise Seamster & Raphaël Charron-Chénier, *Predatory Inclusion and Education Debt: Rethinking the Racial Wealth Gap*, 4 SOC. CURRENTS 199, 199-200 (2017) (describing the targeting of mortgagors and students who borrow to purchase homes or education as "predatory inclusion."). *See also* Kristin Johnson et al., *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 FORDHAM L. REV. 499, 505, 517–21 (2019) (arguing fintech firms may "hardwire predatory inclusion" into financial markets for the "next several generations").

[54] *See* Tamara K. Nopper, *Digital Character in the "Scored Society": FICO, Social Networks, and the Competing Measurements of Creditworthiness, in* CAPTIVATING TECHNOLOGY: RACE, CARCERAL TECHNOSCIENCE, AND LIBERATORY IMAGINATION IN EVERYDAY LIFE 170, 170-188 (Ruha Benjamin ed., 2019), (coining and analyzing the concept of "digital character").

[55] *See*, *e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 13 (2014).

[56] *See*, *e.g.* Alex P. Miller, *Want Less-Biased Decisions? Use Algorithms*, HARV. BUS. REV. (July 26, 2018), https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms [https://perma.cc/8PFS-4MGE].

[57] 15 U.S.C. §§ 1691 et seq. The ECOA applies to consumer and commercial credit.

[58] 42 U.S.C. §§ 3601 et seq.

[59] *See* NAT'L CONSUMER LAW CTR., *supra* note 48 (noting African American, Latinx, and Asian consumers have lower credit scores as a group than whites).

segregation in housing. Even seemingly neutral variables, when used alone or in combination, can correlate with race, ethnicity and other prohibited factors. Learning algorithms, processing large volumes of information, will likely pick up subtle, but statistically significant patterns that correlate with race and other protected characteristics and replicate existing bias.[60] Machine learning algorithms may also analyze variables that engineers did not intend them to analyze.[61] Overall, patterns in alternative credit data can be mined to extract race, ethnicity or other protected characteristics and produce discriminatory outcomes.

Any data used for credit decisions must comply with the ECOA and the FCRA, which at a minimum mandate that the data used be accurate and predictive of creditworthiness.[62] Yet Big Data's records are often inaccurate. For example, an examination of consumer reports generated by eBureau, which has since been acquired by TransUnion, revealed that the underlying information used to assess income and education level was incomplete and primarily gathered without the consumer's knowledge.[63] Moreover, these reports provided no definitive guidance or explanation of how they measure creditworthiness.

The use of alternative data combined with sophisticated algorithms, especially machine learning algorithms, in online marketing and underwriting also raises concerns regarding price discrimination, redlining and steering. Steering occurs online when a consumer is directed towards or away from a loan product or feature because of his race, gender or other prohibited characteristic, rather than based on an applicant's need or other legitimate factor.[64] For example, a creditor may steer limited English proficient (LEP) consumers to a different range of products than non-LEP borrowers.[65] Digital redlining occurs when a creditor provides unequal access to credit or unequal terms of credit based on prohibited characteristics.[66] Data-driven marketing that targets consumers based on prohibited characteristics may engage both forms of discrimination.

Alternative data and analytics have enabled creditors to target people of color and those living in low-income neighborhoods with high-cost loans, including payday loans and subprime

---

[60] *See* Moritz Hardt, *How Big Data is Unfair, Understanding Unintended Sources of Unfairness in Data Driven Decision Making*, MEDIUM (Sept. 26, 2014), http://www.cs.yale.edu/homes/jf/HardtHowBigDataIsUnfair.pdf; Andrew Selbst, *A New HUD Rule Would Effectively Encourage Discrimination by Algorithm*, SLATE (Aug. 19, 2019), https://slate.com/technology/2019/08/hud-disparate-impact-discrimination-algorithm.html.

[61] Johnson et. al., *supra* note 53 at 510.

[62] ECOA, 15 U.S.C. § 1691 et seq.; FCRA, 15 U.S.C. § 1681 et seq.

[63] NAT'L CONSUMER LAW CTR., BIG DATA, A BIG DISAPPOINTMENT FOR SCORING CONSUMER CREDITWORTHINESS 18, (2014), https://www.nclc.org/issues/big-data.html.

[64] Carol Evans, Board of Governors of the Federal Reserve System, *From Catalogs to Clicks: The Fair Lending Implications of Targeted, Internet Marketing*, Consumer Compliance Outlook (Third Issue 2019) at 4.

[65] *See* CFPB, Supervisory Highlights, Issue 13 (Oct. 2016), http://s3.amazonaws.com/files.consumerfinance.gov/f/documents/Supervisory_Highlights_Issue_13__Final_10.31.16.pdf.

[66] *Id.*

mortgages.[67] Such algorithmic profiling also leads to online price discrimination, raising the price of goods and services for consumers in low-income, less technologically-enabled households. The recent action against Facebook by the Department of Housing and Urban Development (HUD) highlighted the discriminatory impact of these targeted advertising and marketing practices. The data used to target Facebook users was unwittingly provided through the actions of users, and those associated with them, on and off the platform.[68] Such behavioral data enabled Facebook to classify users based on protected characteristics and invited advertisers to discriminatorily target or exclude housing-related ads to users based on these imputed protected traits.

Concerns about this form of discrimination extend beyond underwriting to how credit is priced. For example, consumers may be directed to subprime credit cards based on personal characteristics, even though they could qualify for more competitive rates. In the mortgage context one study noted that fintech lenders reduced but did not erase discriminatory lending patterns, particularly with respect to the pricing of loans.[69] Latinx and African American borrowers paid 7.9 and 3.6 basis points more in interest for home purchase and refinance mortgages respectively because of discrimination. These magnitudes represent 11.5% of lenders' average profit per loan.[70]

Additionally, advocates are concerned about the lack of transparency inherent in many of the machine learning models that limit disclosure of the justification for credit based decisions. The ECOA and FCRA notice provisions require that creditors provide credit applicants with notices stating the reasons for credit denial or for taking other adverse actions on an application. These notices may provide clues to help uncover whether the creditor's decision was in fact, discriminatory.

The ECOA notice requirement was designed to fulfill the dual goals of consumer protection and education.[71] Regulation B, which implements ECOA, requires creditors to provide a statement of specific reasons for the action taken or a disclosure of the applicant's right to request a statement of such reasons, with the name, address, and telephone number of the person or office from which the statement of reasons can be obtained.[72] The reasons disclosed must

---

[67] Comment from Nathan Newman, Research Fellow, New York Univ. Information Law Institute, to FTC (Aug. 2014), https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf.
[68] HUD v. Facebook, Charge of Discrimination, FHEO No. 01-18-0323-8 at paragraph 12.
[69] Robert Bartlett, Adair Morse, et al., *Consumer Lending Discrimination in the Fintech Era, National Bureau of Economic Research*, Working Paper 25943 (June 2019), https://www.nber.org/papers/w25943.
[70] *Id.*
[71] Fischl v. Gen. Motors Acceptance Corp., 708 F.2d 143, 146 (5th Cir. 1983).
[72] Reg. B, 12 C.F.R. § 1002.9(a)(3)(i)(B). *See also* Curley v. JP Morgan Chase Bank, 2007 WL 1343793 (W.D. La. May 7, 2007) (discussing the provision), aff'd, 261 Fed. Appx. 781 (5th Cir. 2008).

relate to and accurately describe those factors actually reviewed, considered, or scored.[73] No factor that was a principal reason for the adverse decision may be excluded, even if the relationship of that factor to creditworthiness may not be clear to the applicant.[74]

The notices required by Regulation B raise fundamental transparency issues. Under Regulation B, consumers are statutorily entitled to know what type of information is being used to assess them and how that information is being used. However, where complex algorithms are used based not on standard underwriting factors, but rather unknown alternative data, it is impossible to know exactly what factors were used and how they were used to determine a consumer's creditworthiness. Opaque algorithms which fail to apprise a consumer of the specific and accurate reasons for the credit denial undermine the legislative intent of ECOA and could lead to discriminatory conduct by creditors. Artificial intelligence and machine learning must not be used to reinforce existing discriminatory conduct.[75]

Existing partnerships between IDIs and surveillance-based technology companies have already raised unique, specific concerns. For instance, the new Apple Card — offered in partnership with Goldman Sachs — is currently the subject of a New York State investigation for gender discrimination complaints.[76] Amazon now offers credit cards in tandem with Synchrony Bank, formerly GE Capital Retail Bank, which the Consumer Financial Protection Bureau (CFPB) ordered to provide an estimated $225 million in relief to consumers harmed by illegal and discriminatory credit card practices.[77] A new checking account partnership between Google and Citibank has drawn criticism from privacy advocates, who argue Google wants to sell or share financial data for targeted advertisement or other purposes.[78]

The FDIC Should Consider Links Between Financial Data Collection and Law Enforcement

In assessing whether certain innovations are appropriate for IDIs, the FDIC must bear in mind that new technologies may endanger our civil liberties in new ways. "Bulk" financial

[73] Official Interpretations of Reg. B, 12 C.F.R. pt. 1002, supp. I, § 1002.9(b)(1)-2.
[74] *Id.* at § 1002.9(b)(2)-4.
[75] For a list of studies, *see* NAT'L CONSUMER LAW CTR., *supra* note 48.
[76] Neil Vigdor, *Apple Card Investigated After Gender Discrimination Complaints*, N.Y. TIMES (Nov. 10, 2019), https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html.
[77] Kate Rooney, *Amazon launches a credit card for the 'underbanked' with bad credit,* CNBC (Jun. 10, 2019), https://www.cnbc.com/2019/06/10/amazon-launches-a-credit-card-for-the-underbanked-with-bad-credit.html; CFPB, CFPB Orders GE Capital to Pay $225 Million in Consumer Relief for Deceptive and Discriminatory Credit Card Practices (Jun. 19, 2014), https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-ge-capital-to-pay-225-million-in-consumer-relief-for-deceptive-and-discriminatory-credit-card-practices/.
[78] John Constine, *Leaked pics reveal Google smart debit card to rival Apple's*, TECHCRUNCH (April 17, 2020), https://techcrunch.com/2020/04/17/google-card/.

surveillance eventually creates a detailed picture of our most private social, familial, romantic, religious, and political activities. Data about a single transaction can be linked to purchase history, creating a "picture of the person behind the payment."[79] A massive data broker industry connects data regarding our finances to data about our employment, marital status, homeownership status, medical conditions, and even our interests and hobbies.

Law enforcement authorities use sensitive corporate data, including financial data, to target vulnerable communities.[80] As a general matter of course, "surveillance-as-a-service" companies sell data, including financial data, to local police departments.[81] Historically, the National Security Agency (NSA) and other federal law enforcement agencies have exploited corporations' growing troves of records.[82] Indeed, tech companies have a long history of spying on users at the behest of government agencies (which disregard court rulings as to the unconstitutionality of their practices).[83] It would be unwise for regulators to divorce analysis of corporate surveillance from government surveillance.[84]

As Justices Thurgood Marshall and William Douglas warned in the 1970s, technology that allows for faster and better banking has led to easier law enforcement access to depositor data.[85] While it is true that bank account holders are protected by statutes like the Right to Financial Privacy Act of 1978, this law only requires government agencies provide individuals with a notice and an opportunity to object before a bank discloses personal information to the federal government.[86] There is also a general carveout for certain law enforcement, rendering the law more of a procedural rather than substantive barrier to violations of civil liberties.[87]

---

[79] Albert Fox Cahn & Melissa Giddings, *In the Age of COVID-19, the Credit Card Knows All*, Surveillance Technology Oversight Project - Urban Justice Center (May 18, 2010), https://www.stopspying.org/latest-news/2020/5/18/in-the-age-of-covid-19-the-credit-card-knows-all.

[80] *See*, *e.g.,* Simone Browne, Dark Matters: On the Surveillance of Blackness 10-29 (2015) ("Surveillance is nothing new to black folks. It is the fact of antiblackness."); Virginia Eubanks, Automating Inequality 1-38 (2017) (detailing how programs have demanded poor people sacrifice their rights to privacy and self-determination); Cohen, *supra* note 17, at 61 (noting law enforcement agenices have conducted prolonged, intrusive surveillance of Muslim and Latinx communities, relying on corporate communications metadata).

[81] *See, e.g.,* Shoshana Zuboff, The Age of Surveillance Capitalism 37 (2019).

[82] *See, e.g.,* Cohen, *supra* note 9, at 238-242 (arguing bulk collection and analysis of data generated by networked communications intermediaries have become "pillars" of state surveillance).

[83] *See* Sean Vitka, Demand Progress, "Institutional Lack of Candor" A Primer on Recent Unauthorized Activity by the Intelligence Community (Sept. 27, 2017), https://s3.amazonaws.com/demandprogress/reports/FISA_Violations.pdf.

[84] *See, e.g.,* Cohen, *supra* note 9, at 43 (describing a "surveillance-innovation complex", wherein the state and private sector producers of surveillance technologies form a "symbiotic relationship").

[85] Dean Galaro, *A Reconsideration of Financial Privacy and United States v. Miller*, 59 S. Tex. L. Rev. 31, 54 (2017).

[86] *See* 12 U.S.C. § 3404.

[87] *See id.* at §§ 3406-08 (financial institutions can disclose customer records in response to a search warrant, subpoena, or written request from a government authority).

All financial institutions must comply with Title III of the USA PATRIOT Act, which requires they implement robust customer identification programs, commonly labeled "know your customer" (KYC) provisions.[88] Financial institutions must generally assist police investigations requiring financial information and provide specific information to law enforcement agencies,[89] including by filing "suspicious activity reports" (SARs).[90]

Given these obligations, and the racial injustices perpetrated by law enforcement, we are especially concerned by suggestions that IDIs — on their own initiative or in partnership with tech companies — should collect more geolocation or biometric data.[91] Geolocation data revealed by payment histories is uniquely difficult to anonymize.[92] Privacy and racial justice advocates vehemently oppose the use of biometric tools like facial recognition technology, iris-scanning, and palm prints.[93] Facial recognition software is likely to mislabel or misrecognize members of racial minority groups, especially Black Americans.[94] Yet some tech companies

---

[88] *See*, *e.g.,* Letter from Rep. Tlaib, et al., to the Treas. Sec. Steve Mnuchin, et al., (July 17, 2019), https://tlaib.house.gov/sites/tlaib.house.gov/files/Final_BWM_Regulators.pdf (arguing many Muslim and Arab Americans have been automatically labeled "high-risk" and are therefore unable to maintain access to financial services). For a history of the relevant PATRIOT Act amendments, see, e.g., Maria A. de Dios, *The Sixth Pillar of Anti-Money Laundering Compliance: Balancing Effective Enforcement with Financial Privacy*, 10 BROOK J. CORP. FIN & COM. L. 495 (2016); Cheryl R. Lee, *Constitutional Cash: Are Banks Guilty of Racial Profiling in Implementing the United States Patriot Act?*, 11 MICH. J. RACE & L. 557, 564 (2006) (arguing the Patriot Act 'puts banks in the business of practicing selective enforcement and racial profiling with every transaction, every hour of every business day"); Eric J. Gouvin, *Bringing Out the Big Guns: The USA PATRIOT Act, Money Laundering, and the War on Terrorism,* 55 BAYLOR L. REV. 955 (2003).

[89] The information in the database is accessible by federal, state and local law enforcement agencies, and can be used in investigations. *See*, *e.g.,* Daniel Bush, *How banks and the government keep track of suspicious financial activity*, PBS NEWSHOUR (June 12, 2020), https://www.pbs.org/newshour/politics/how-banks-and-the-government-keep-track-of-suspicious-financial-activity. For further background, see, e.g., Ben Hayes, *Counter-Terrorism, "Policy Laundering," and the FATF: Legalizing Surveillance, Regulating Civil Society*, 14 INT'L J. NOT-FOR-PROFIT L. 5, 19 (2012); Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and the Unlawful Repression of Political Dissent*, 81 OR. L. REV. 1051, 1116 (2002) (noting many companies report being pressured to "turn over customer records voluntarily, in the absence of either a court order or a subpoena, 'with the idea that it is unpatriotic if the companies insist too much on legal subpoenas first.'").

[90] 31 C.F.R. § 1022.320.

[91] *See. e.g,* Letter from Demand Progress et al. to Leaders McConnell and Schumer, Speaker Pelosi and Leader McCarthy: (July 1, 2020), https://s3.amazonaws.com/demandprogress/letters/2020-07-01_Facial_Recognition_Moratorium_and_Divestment_Letter_FINAL.pdf; Alfred Ng, *Facial recognition has always troubled people of color. Everyone should listen*, CNET (June 12, 2020), https://www.cnet.com/news/facial-recognition-has-always-troubled-people-of-color-everyone-should-listen/.

[92] *See, e.g.,* Cahn & Giddings, *supra* note 79.

[93] *See, e.g.*, *A Biometric Backlash Is Underway — And A Backlash To The Backlash*, PYMNTS (May 17, 2019), https://www.pymnts.com/authentication/2019/biometric-backlash-privacy-law/; *Mandatory National IDs and Biometric Databases*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/national-ids (last visited Apr. 25, 2020); de Dios, *supra* note 88, at 501 (describing how prior to September 11, 2001, even non-biometric KYC data collection was widely considered an unacceptable, "massive invasion of financial privacy.").

[94] *See, e.g.,* Victoria Burton-Harris & Philip Mayor, *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart*, ACLU (June 24, 2020), https://www.aclu.org/news/privacy-technology/wrongfully-arrestedbecause.

engaged in financial services are attempting to create entire biometric-based, portable digital identities to substitute for government ID.[95] Although supporters predictably cite "financial inclusion" as a business justification, biometric tools in question have proven to be of limited value in the context of financial services provision.[96] Overall, the general use of this kind of sensitive data not only increases the risk of predation by banks and civil liberties violations by governments, but security breaches by competitors and hackers.[97] NIST has recently established risk-based technical standards for each of the component processes of a digital identity system (enrollment and identity proofing; authentication and lifecycle management; and federation), which are mandatory for the federal government, but only voluntary for the private sector.[98] As part of this effort, it has already tested the accuracy of facial recognition systems in different scenarios.[99] It may be of more service to the FDIC than a private industry-led SSO.

In general, we should question whether specific forms of financial exclusion are in fact technological at their roots. Heightened surveillance may actually stand to chill financial inclusion. FDIC surveys consistently note that many "unbanked" households refuse to open bank accounts due to privacy concerns.[100] While providing increased access to digital financial services is important, a rapid shift to digitization — not to mention the broader "war on cash"[101]

---

[95] *See* LIBRA ASS'N MEMBERS, WHITE PAPER v2.0 (2020), https://libra.org/en-US/white-paper// (last visited June 22, 2020).

[96] *See, e.g.,* ET Bureau, *Aadhaar verdict: Telcos, banks & financial companies may feel the pinch*, THE ECON. TIMES (Sept. 27, 2018), https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-telcos-banks-financial-companies-may-feel-the-pinch/articleshow/65973414.cms (noting that biometric IDs linked to a central registry are still not acceptable for KYC purposes).

[97] *See, e.g.*, Jason Leopold & Jessica Garrison, *US Intelligence Unit Accused Of Illegally Spying On Americans' Financial Records*, BUZZFEED (Oct. 6, 2017), https://www.buzzfeednews.com/article/jasonleopold/Us-Intelligence-unit-accused-of-illegally-spying-on (reporting that FinCEN employees have accused colleagues at the Office of Intelligence and Analysis of illegally collecting and storing private financial records); Aaron Mackey & Andrew Corker, *Secret Court Rules That the FBI's "Backdoor Searches" of Americans Violated the Fourth Amendment*, ELECTRONIC FRONTIER FOUND. (Oct. 11, 2019), https://www.eff.org/deeplinks/2019/10/secret-court-rules-fbis-backdoor-searches-americans-violated-fourth-amendment; Chen Han & Rituja Dongre, *Q&A. What Motivates Cyber-Attackers?*, TECH. INNOV. MGMT. REV. 40, 40-41 (2014), https://timreview.ca/article/838 (describing economic motivations for hacking).

[98] ¶ 155-636 TREASURY REPORTS TO PRESIDENT ON NONBANK FINANCIALS, FINTECH, AND INNOVATION., Fed. Bank. L. Rep. P 155-636.

[99] *See*, *e.g.,* Letter from EFF, Demand Progress et al. to Congressional Leadership (July 1, 2020), https://www.eff.org/files/2020/07/08/2020-07-01_facial_recognition_moratorium_and_divestment_letter_final.pdf; *Face Recognition Vendor Test*, NIST (Apr. 2, 2010), https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt [https://perma.cc/EGQ4-8Y3H]. *See also* Kristin N. Johnson, *Automating the Risk of Bias*, 87 GEO. WASH. L. REV. 1214, 1244 (2019) (discussing NIST and FRT in the broader context of algorithmic bias).

[100] FDIC, NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS, 2017 4, 23-24, https://www.fdic.gov/householdsurvey/. *See also, id.* at 3 (noting Black households are nearly six times more likely to be unbanked than white households, while Hispanic households are nearly five times more likely to be unbanked than white households).

[101] Jay Stanley, *Say No to the "Cashless Future" — and to Cashless Stores*, ACLU (Aug. 12, 2019), https://www.aclu.org/blog/privacy-technology/consumer-privacy/say-no-cashless-future-and-cashless-stores.

— stands to harm low-income people of color in particular. The fintech revolution presumes a certain technological infrastructure (like universal broadband),[102] not to mention a certain level of household financial stability.[103]

Conclusion

The RFI asks what the FDIC can do to "support the financial services industry's development and usage of a standardized approach to the assessment of models or the due diligence of third-party providers of technology and other services."[104] As a general matter, we believe the FDIC and other banking regulators should set standards and develop their own facilities in this arena. If banking regulators truly aim to reduce regulatory and operational uncertainty, they will not accomplish this goal by inserting additional decision-makers — shielded from public scrutiny — into the regulatory process. Banking regulators should clarify the extent to which they are experiencing difficulty understanding contemporary information technology. If the extent is great, NIST and other public institutions are available to assist them.

Privatization of standard-setting would only permit IDIs to further engage in activities that may present risks that are not fully understood by banking regulators.[105] This is especially important because while providing data processing, data storage, and data transmission services is permissible for Bank Holding Companies (BHCs) and their subsidiaries,[106] it is questionable how much Big Data collection would actually be used to improve banking and how much would be used for other business endeavors. As a general matter, we strongly agree with other recent commenters that banking regulators should respect Congress's strongly articulated purpose of separating banking and commerce.[107]

In any format, we oppose the provision of banking privileges to companies that do not take deposits or that use technologies that could threaten our safety and wellbeing, especially for communities of color. Some sorts of digital activities should be kept out of the financial system,

---

[102] *See*, *e.g.*, Terri Friedline, *An Open Internet is Essential for Financial Inclusion, FinTech Revolution*, HUFF. POST (Dec. 14, 2017), https://www.huffpost.com/entry/an-open-internet-is-essential-for-financial-inclusion_b_5a3345dce4b0e1b4472ae520.
[103] *See* Stanley, *supra* note 101.
[104] RFI at 13.
[105] *See, e.g,* Elizabeth J. Upton, *Chartering Fintech: The OCC's Newest Nonbank Proposal*, 86 GEO. WASH. L. REV. 1392, 1409 (2018).
[106] *See* 12 U.S.C. § 1843(a)(2).
[107] *See* Comment from Arthur E. Wilmarth, Jr., Prof. of Law, Geo. Wash. Univ. L. Sch., to FDIC (Apr. 10, 2020), https://www.fdic.gov/regulations/laws/federal/2020/2020-parent-companies-of-industrial-banks-3064-af31-c-002.pdf.

period.[108]

We echo Iowa Law School professor Chris Odinet in arguing that the way regulators have gone about addressing financial technology has likely impeded innovation.[109] This is not because they have failed to sufficiently listen to the tech industry. It is because regulators are moving forward on their own, without taking the time to consult with the states or Congress.

The "new language of financialization" will be defined by "privileged access to data."[110] Any such privileges need to be paired with powerful guardrails and responsibilities. At a time of great economic, political, and social uncertainty, banking regulators need to be especially vigilant regarding threats to the integrity of financial institutions.[111] Policymakers must avoid being swayed by general promises of 'innovation' and create systems for real accountability on behalf of the public.

We have attempted to summarize our thoughts on a number of financial technology topics, but these are incomplete. Other public interest organizations that have not had the capacity to comment right now -- given the pandemic and global depression -- also have important perspectives to offer. We therefore urge the FDIC not to rush any fintech initiatives and to seek more public comment on these topics before moving forward.

We appreciate the opportunity to comment on this RFI. If you have questions, please contact Raúl Carrillo (Fellow, AFR Education Fund; Policy Counsel, DPEF) at raul@ourfinancialsecurity.org.

Respectfully submitted,

Americans For Financial Reform Education Fund
Demand Progress Education Fund

---

[108] *See, e.g.,* Graham Steele, *Facebook's Libra cryptocurrency is part of a disturbing financial trend,* WASH. POST (Aug. 12, 2019), https://www.washingtonpost.com/outlook/2019/08/12/facebooks-libra-cryptocurrency-is-part-disturbing-financial-trend/.
[109] Pedersen, *supra* note 41.
[110] COHEN, *supra* note 9, at 233.
[111] *See, e.g.,* ¶ 157-019 CIGFO REPORT SHOWS CYBERSECURITY, CORONAVIRUS MAJOR ISSUES FOR FEDERAL REGULATORS., Fed. Bank. L. Rep. P 157-019.