



August 3, 2020

Brian Brooks  
Acting Comptroller of the Currency  
Office of the Comptroller of the Currency  
400 7th Street, SW., suite 3E-218  
Washington, DC 20219.

***Re: National Bank and Federal Savings Association Digital Activities, Docket ID  
OCC-2019-0028***

Dear Acting Comptroller Brooks:

Consumer Reports<sup>1</sup> (CR) writes today in response to the Office of the Comptroller of the Currency (OCC) advanced notice of proposed rulemaking (ANPR) on National Bank and Federal Savings Association Digital Activities. While the digital, and in particular mobile, interfaces are newer ways in which financial institutions deliver products and services, and engage with their customers, the need for and tenets of consumer financial protection remain the same. Consumer protection is a result of ensuring appropriate oversight, financial soundness, and duties to protect consumers. We urge the OCC, as it reviews regulations on bank digital activities, to focus on ensuring consumer protection, rather than ensuring “its regulations continue to evolve with developments in the industry.”<sup>2</sup> In particular, we urge the OCC to redouble its efforts to ensure consumer financial data privacy, enhance its scrutiny of artificial intelligence and machine learning in financial services with an aim to prevent discrimination and bias, and to ensure other consumer protections.

Consumer Reports (CR) has a long history of working to ensure financial innovation, and particularly digital finance, is safe. People need to spend, save and borrow with confidence,

---

<sup>1</sup> Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumer Reports works for pro-consumer policies in the areas of financial services and marketplace practices, antitrust and competition policy, privacy and data security, food and product safety, telecommunications and technology, travel, and other consumer issues, in Washington, DC, in the states, and in the marketplace. Consumer Reports is the world’s largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

<sup>2</sup> <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-76a.pdf> at 1

regardless of whether those interactions take place in a bank branch, online or via an app. CR called for prepaid protections in the early 2000s,<sup>3</sup> was a leader in passing state data breach notification laws,<sup>4</sup> documents the problems with mobile payments,<sup>5</sup> and advocates for fundamental protections for cryptocurrency users.<sup>6</sup> In 2018, Consumer Reports rated peer-to-peer payment services, including Apple, Square’s Cash app and Venmo.<sup>7</sup> With the launch of CR’s Digital Lab in 2019, Consumer Reports continues to make the safety and security of digital financial services an essential part of our work for a fair, just and safe marketplace.

### **The OCC Principles Do Not Go Far Enough to Ensure Consumer Protection**

In the ANPR is a description of the principles “that guide the OCC’s approach to its regulatory framework in the context of technology and innovation.”<sup>8</sup> The first principle is that regulation should be technology neutral. While we understand the desire to have regulations that do not change as quickly as technology, we urge the OCC to remember that even if regulation is technology- neutral, technology itself is not. Technology is often first directed at and used against the interests of people of color and people with lower wealth.<sup>9</sup> As discussed in more detail below, newer technologies may pose direct risks to consumers with the least power to avoid them. We therefore urge the OCC, rather than focusing on staying “technology neutral,” to make a critical assessment of newer technologies, and keep consumer protection top of mind when doing so.

The second OCC principle, that regulation should promote privacy and consumer protection, urges transparency and informed consent. We agree that promoting privacy is critical, disclosure and consumer controls are not enough. For reasons discussed in more detail below, the burden should not fall solely on consumers to navigate obscure technical and legal language to make choices about their safety or privacy. There need to be firm rules on data collection, sharing and storage. And some data collection should simply be off limits to financial service providers.

---

<sup>3</sup> Consumer Reports, Prepaid Cards, How They Rate <https://advocacy.consumerreports.org/research/prepaid-cards-how-they-rate-2/>.

<sup>4</sup> Consumer Reports, Another Week, Another Identity Theft Scandal, [https://advocacy.consumerreports.org/research/another\\_week\\_another\\_identity\\_theft\\_scandal/](https://advocacy.consumerreports.org/research/another_week_another_identity_theft_scandal/).

<sup>5</sup> Michelle Jun, Mobile Pay or Mobile Mess, <https://advocacy.consumerreports.org/wp-content/uploads/2013/02/Mobile-Pay-or-Mobile-Mess.pdf>.

<sup>6</sup> Consumers Union and National Consumer Law Center, comments on the Draft Model Regulatory Framework (“Draft Framework”) for State Virtual Currency Regulatory Regimes, <https://www.csbs.org/sites/default/files/2017-11/Consumers%20Union%20and%20NCLC%20Framework%20Comment.pdf>.

<sup>7</sup> Why Apple Pay Is the Highest-Rated Mobile P2P Payment Service, <https://www.consumerreports.org/digital-payments/mobile-p2p-payment-services-review/>.

<sup>8</sup> <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-76a.pdf> at 10.

<sup>9</sup> *See for example*, Charlton Mcllwain, Of course technology perpetuates racism. It was designed that way, <https://www.technologyreview.com/2020/06/03/1002589/technology-perpetuates-racism-by-design-simulmatics-charlton-mcilwain/>, and Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.

The third OCC principle, that “regulations on digital activities should be principle based, rather than prescriptive,” presumes that technological innovation will outpace the ability of rules to keep up with risks. However, there is very little true product innovation. Most “fintech” offerings fall within established legal definitions of products and services for deposit-taking, money transmission or lending. The novelty in digital finance is the scope of data collection and the uses that data are put to, and while we agree, as noted above, that privacy needs to be a focus, consumer protection requires strong rules. The OCC should ensure that there are clear rules rather than relying on a principles-based approach. Well-intentioned but vague principles leave the door open to lax oversight and consumer harm. To prevent harm to individuals and the financial system, there must be mandatory, enforceable standards for both safety and soundness as well as consumer protection. Consumer protection should not be left to the chance of weak implementation of vague principles.

### **Digital Financial Service Providers Should Practice Data Minimization**

Digital innovation brings many benefits to consumers. However, digital financial services -- with its prevalent and expansive collection, monetization, and use of personal consumer data -- can come into conflict with the right to privacy. Some data collection is necessary and appropriate for baseline product usability, but often digital financial data collection far exceeds this baseline. Service providers must be transparent about their data collection, sharing and selling practices, and wherever possible, consumers should be able to make choices about the information that companies are allowed to collect about them. However, consumers shouldn't bear the entire burden of protecting their privacy through settings and controls.

Surveillance is a privacy harm, and consumers have a privacy interest in controlling commercial collection of their personal information, as CR's Director of Privacy and Technology Policy Justin Brookman has written.<sup>10</sup> Digital financial service providers justify their all-encompassing surveillance of users in the name of “analytics” or “product improvement.” Providers also reserve broad rights to use user data for unrelated purposes, including targeted advertising. Recent CR research illustrates how far reaching the data collection of some financial service providers is. In a CR review of digital savings apps, we found indicia that the service providers, and the data aggregators these companies rely on, collect and share user data well outside what a user would reasonably expect.<sup>11</sup> As part of its efforts in digital finance, the OCC should consider ways it can encourage financial institutions to practice data minimization and deletion of consumer data. For example, CR research has shown that financial service providers sometimes hold user information indefinitely, making these companies rich targets for data breaches, subpoenas or legal procedures, or insider threats. In general, the more data collected, the more valuable data that is, the more likely someone will want to steal it. Some

---

<sup>10</sup> Justin Brookman and G.S. Hans, Why Collection Matters: Surveillance as a *De Facto* Privacy Harm, <https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf>.

<sup>11</sup> Consumer Reports comments to the Consumer Financial Protection Bureau's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, [https://files.consumerfinance.gov/f/documents/cfpb\\_tetreault-statement\\_symposium-consumer-access-financial-records.pdf](https://files.consumerfinance.gov/f/documents/cfpb_tetreault-statement_symposium-consumer-access-financial-records.pdf).

primary data collection and use, and some secondary sharing should be out-of-bounds due to the sensitivity of the data or the potential for discrimination or abuse. For example, with the possible exception of assessing actuarial risk for insurance, financial services providers have no reason to collect or share consumer medical information; and social media, including user generated content and contacts, should not be allowed for credit decisioning. In short, the OCC should work to ensure that data is not weaponized against consumers.

### **The OCC Should Issue Rules to Ensure Algorithmic Accountability**

The data collected about consumers is routinely processed by algorithms that make decisions about them. In financial services, algorithms are routinely used to determine auto insurance rates, creditworthiness, willingness to pay, and now as a result of the pandemic, we are seeing new ways in which consumer data is processed to assess people. For example, in addition to its FICO score used for credit decisioning, FICO now offers a “Resilience Index” which lenders can “leverage” to “rank-order consumers by sensitivity to economic stress.”<sup>12</sup>

Proponents advocate for the use of artificial intelligence in financial services, claiming it can “reduce human biases and errors.”<sup>13</sup> Algorithms are often positioned to consumers, regulators and financial institutions as expanding access to financial services<sup>14</sup> and/or decreasing bias in the provision or pricing of services.<sup>15</sup> For example, lender and bank service provider Upstart’s mission “is to enable effortless credit based on true risk.”<sup>16</sup> Upstart claims it uses “more than” 1,500 data points as part of its algorithmic decision making.<sup>17</sup> It also makes its Credit Decision API available to banks.<sup>18</sup> An analysis by the Student Borrower Protection Center (SBPC) earlier this year raised questions about the fairness of Upstart’s decision making.<sup>19</sup> For example, the SBPC reported that borrowers who refinance with Upstart may pay a penalty for having attended an historically black college or university.<sup>20</sup>

Claims of objectivity and proof notwithstanding, algorithms can and do exacerbate bias or have unexpected discriminatory effects, as numerous examples have demonstrated.<sup>21</sup> While there

---

<sup>12</sup> <https://www.experian.com/consumer-information/fico-resilience-index>

<sup>13</sup> Oliver Wyman, Insights Artificial Intelligence Applications in Financial Services, <https://www.oliverwyman.com/our-expertise/insights/2019/dec/artificial-intelligence-applications-in-financial-services.html>.

<sup>14</sup> See for example, LendUp: “We consider all types of credit history. Just because your credit score may be “not-so-great” doesn’t mean you can’t get approved.” <https://www.lendup.com/>

<sup>15</sup> “Artificial intelligence (AI) presents an opportunity to transform how we allocate credit and risk, and to create fairer, more inclusive systems.” Aaron Klein, Brookings Institution, Reducing bias in AI-based financial services, <https://www.brookings.edu/research/reducing-bias-in-ai-based-financial-services/>.

<sup>16</sup> <https://www.upstart.com/about>

<sup>17</sup> <https://www.upstart.com/blog/introducing-credit-decision-api>

<sup>18</sup> <https://www.upstart.com/for-banks/credit-decision-api/>

<sup>19</sup> Student Borrower Protection Center, Educational Redlining, <https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf>.

<sup>20</sup> *Id.* at 4.

<sup>21</sup> ProPublica and Consumer Reports: Auto Insurers Charging Higher Rates in Some Minority Neighborhoods, First-of-its-kind analysis finds pricing disparities between minority and non-minority neighborhoods cannot be explained by average risks, suggests potential redlining,

are laws that prohibit discrimination, there are not laws in place that ensure sufficient transparency, testing or accountability of algorithms. As consumers lack any means to correct erroneous conclusions made by algorithms, or any recourse to object to the use of an untested and undisclosed algorithm to make inferences or decisions about them, rules governing their use are needed. CR staff have specific suggestions for improving algorithmic accountability, including the following:

- **The use of algorithms should be transparent to the end users.** When algorithms make decisions about consumers the individual should have notice that an algorithm was used.
- **Algorithmic decision-making should be testable for errors and bias.** Algorithms should be able to be tested by outside researchers and investigators.
- **Algorithms should be designed with fairness and accuracy in mind.** Companies should not simply rely on outsiders to detect problems with their algorithms; instead, companies should be required to plan for and design to avoid adverse consequences at all stages of the development of algorithms.
- **The data set used for algorithmic decision-making should avoid the use of proxies.** Algorithms can only serve to address the question posed to them. When possible, algorithms should avoid the use of unnecessary proxies like zip codes, education data, or marital status as these can also serve as proxies for prohibited factors such as race.
- **Algorithmic decision-making processes that could have significant consumer consequences should be explainable.** In some cases, algorithms are programmed to learn or evolve over time, such that a developer might not know why certain inputs lead to certain results. This could lead to unfair results if there is no meaningful accountability for how decisions are made. If an algorithm is (1) used for a significant purpose, like the determination of a credit score and (2) cannot be sufficiently explained, then the process should not be used.<sup>22</sup>

If regulators fail to enact sufficient safeguards around the use of algorithms, artificial intelligence and machine learning, the risk is that these systems will perpetuate and further entrench existing inequities and biases.<sup>23</sup> The OCC should move forward with rulemaking for algorithmic decision making in financial services to prevent this outcome.

---

[https://www.consumerreports.org/media-room/press-releases/2017/04/propublica\\_and\\_consumer\\_reports\\_auto\\_insurers\\_charging\\_higher\\_rates\\_in\\_some\\_minority\\_neighborhoods11/](https://www.consumerreports.org/media-room/press-releases/2017/04/propublica_and_consumer_reports_auto_insurers_charging_higher_rates_in_some_minority_neighborhoods11/).

<sup>22</sup> Justin Brookman, Katie McInnis, Re: Post-Hearing Comments on Algorithms, Artificial Intelligence, and Predictive Analytics for the Federal Trade Commission's Hearings on Competition and Consumer Protection in the 21st Century on November 13-14, 2018, FTC-2018-0101, *available at* <https://advocacy.consumerreports.org/wp-content/uploads/2019/02/CR-AI-FTC-comments.pdf>.

<sup>23</sup> Kristin Johnson, Frank Pasquale, and Jennifer Chapman, Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation, 88 Fordham L. Rev. 499 (2019). Available at: <https://ir.lawnet.fordham.edu/flr/vol88/iss2/5>.

## Basic Consumer Protections for Cryptocurrency Are Needed

Cryptocurrency and blockchain (aka distributed ledger) companies have made many claims about their ability to increase financial inclusion.<sup>24</sup> The Libra project, for example, is justified by Facebook with the dubious claim that it will empower billions of people.<sup>25</sup> The reality is that the reasons consumers are outside the financial mainstream in the United States are largely structural. Nothing about cryptocurrency fixes this, nor will any app or digital wallet.

Cryptocurrency scams and fraud are rampant, and hacking of wallets and exchanges, where virtual currencies are stored, is common. These products and services should not be tested on consumers with the least cushion in their financial lives.

There are open questions about how the law applies to blockchain. The public, “immutable” blockchain has been put forward as a means of solving the problem of privacy,<sup>26</sup> intellectual property rights,<sup>27</sup> and voter fraud,<sup>28</sup> among other things, but in financial services blockchain may be used for back-of-the-house services, such as automating compliance,<sup>29</sup> and for payments.<sup>30</sup> In financial services, the lack of a shared vocabulary to describe the technology and its capabilities raises questions about the appropriateness of its use in critical systems.<sup>31</sup> Moreover, core claims about the technology, for example that blockchain ledgers are immutable and that governance is decentralized, are very much in doubt.<sup>32</sup> The OCC should proceed with caution in its approach to blockchain and its use in financial services. A good first step is to ensure the accuracy of both terms used to describe blockchain and the validity of claims made about it are based in evidence and not dependent on the wishful thinking of proponents.

---

<sup>24</sup> See for example, Swell 2019: Dr. Raghuram Rajan on Enabling Financial Inclusion with Blockchain and Digital Assets, <https://ripple.com/insights/swell-2019-dr-raghuram-rajan-enabling-financial-inclusion-with-blockchain-and-digital-assets/>

<sup>25</sup> “The Libra Association’s mission is to enable a simple global payment system and financial infrastructure that empowers billions of people.” Cover letter to the revised Libra white paper, <https://libra.org/en-US/white-paper/#cover-letter>.

<sup>26</sup> <https://www.theguardian.com/commentisfree/2018/mar/21/blockchain-privacy-data-protection-cambridge-analytica>

<sup>27</sup>

<https://www.forbes.com/sites/andrewrossow/2018/07/24/how-can-we-make-intellectual-property-rights-smarter-with-the-blockchain/#506c111c85ec>

<sup>28</sup> Brookings, How Blockchain Could Improve Election Transparency, <https://www.brookings.edu/blog/techtank/2018/05/30/how-blockchain-could-improve-election-transparency/>

<sup>29</sup> <https://www.mortgagebankermag.com/compliance/regulatory-compliance-efficiency-utilizing-blockchain/>

<sup>30</sup> For example, RippleNet for cross border payments, <https://ripple.com/>.

<sup>31</sup> Walch, Angela, Blockchain's Treacherous Vocabulary: One More Challenge for Regulators (July 1, 2017). Journal of Internet Law, Vol. 21, No. 2, Aug. 2017., Available at SSRN: <https://ssrn.com/abstract=3019328>

<sup>32</sup> Walch, Angela, Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems (January 30, 2019). Crypto Assets: Legal and Monetary Perspectives (OUP, Forthcoming), Available at SSRN: <https://ssrn.com/abstract=3326244>.

Right now and in the absence of action from either Congress or Consumer Financial Protection Bureau, the few consumer protections that cryptocurrency users have are mostly found in state money transmitter laws. These state laws lack the types of payments protection found in federal law. To date, the Consumer Financial Protection Bureau has declined to opine on whether Reg E applies to cryptocurrency wallets. Similarly, there is no federal deposit insurance for cryptocurrency. Given that service providers position cryptocurrency and blockchain as solutions for populations either underserved or abused by the current financial services industry, it is imperative that basic protections for consumers are in place before these products become widely used. The OCC should work with other federal financial regulators to develop appropriate consumer protections for cryptocurrency and blockchain.

### **Conclusion**

With the rise of digital finance comes additional consumer risks. The privacy harms of data collection, and the potential discriminatory effects of algorithmic decision making are urgently in need of attention from federal financial regulators. We urge the OCC to work with others to establish clear rules to ensure fair financial services.

Respectfully submitted,

Christina Tetreault  
Manager, Financial Policy