Correcting the Record on the CFPB's Open Banking Rule

Consumer Financial Protection Bureau Director Rohit Chopra made two appearances yesterday to announce the release of the Bureau's latest rulemaking, known as Section 1033. The rule governs how consumers access their financial data and how that data is protected. **The Director made several statements in his remarks that warrant clarification:**

Director Chopra: "[T]he rule also strengthens protections by accelerating the shift away from the industry practice known as 'screen scraping.'" … "By moving things to more secure sharing, we are going to be able to sunset this practice of screen scraping…"

Fact: There is nothing in the rule that would "sunset" the practice of screen scraping. The CFPB suggests in the preamble that it *could* regulate screen scraping in the future under its existing authority; however, the final rule does nothing to legally prohibit screen scraping practices. Many data aggregators will continue to rely on unsafe practices such as screen scraping to obtain account and transaction data, often collecting and retaining more information than is needed to offer a desired product or service.

Director Chopra: "Banks are responsible for securing data, ***and so are fintechs***. You're right, we need to make sure that everyone is being watched to make sure that they are adhering to those standards of the law, but banks and nonbanks alike are required to have data security standards to not allow those leakages…"

Fact: The CFPB takes no accountability for the oversight or supervision of data recipients (e.g., fintechs) under this rule. That means that banks are forced to police whether data recipients are employing appropriate security measures. Yet, the rule is not even clear when banks may be able to deny access to third parties based on legitimate security concerns.

The Treasury Department issued a report in 2022 finding that "...there is virtually no regulatory oversight of data aggregators' storage of consumer financial information akin to the supervision of [banks'] data security." Giving third parties access to a customer's bank account without regulatory oversight undermines existing legal protections, such as the Gramm-Leach-Bliley Act, rigorous bank exams under FFIEC guidelines and various state and international data security and privacy laws.

Director Chopra: "[Fraud] will happen in any circumstance in a digital economy."

Fact: The CFPB should have no higher priority than protecting consumers. The Bureau's Director dismissing fraud concerns as the cost of doing business in a digital economy is an abdication of responsibility and unacceptable. Fraud is a growing problem in America. However, the rule exacerbates the threat of fraud and scams. For example, the rule requires banks to provide information to third parties to allow them to initiate payments from consumers' accounts.

The latest data from the Federal Trade Commission estimates that there were over 2.6 million fraud reports in 2023, representing over $10 billion in reported losses, a 14% increase over 2022. The rule exposes customers' funds to unacceptable risks by requiring banks to share sensitive account information. Without proper oversight and supervision of aggregators and third parties, the chances of bad actors gaining access to data from entities with weak security practices rise. Exposure to account and routing numbers, along with transaction data, could provide fraudsters with all the details they need to initiate unauthorized transfers and engage in other malicious activities.

Director Chopra: "It can be a real pain to switch your bank account or your credit card or other financial service, and what these new rules will do is inject even more control for consumers in the market by making it easier to move your money, to switch and to fire that bank or financial company that is not serving you well."

Fact: Industry-led efforts already empower millions of Americans to move their money and safely share data. The system is working and is continuously evolving to allow consumers to share their data safely. The largest banks currently facilitate billions of secure data transfers every month and are active contributors to industry standard-setting bodies like the Financial Data Exchange.