PUBLICATION

CFPB Proposes Rule to Regulate Data Brokers Selling Sensitive Information

Authors: Alexander Frank Koskey, III, Matthew George White, Madison J. McMahan
December 13, 2024

In today's digital landscape, data brokers are like modern-day gold miners, sifting through the intimate details of our lives – our addresses, financial records, Social Security numbers – and quietly turning that information into profit. Most of us never asked for this arrangement, yet here we are, with personal data fueling a booming, largely unregulated industry.

The Consumer Financial Protection Bureau (CFPB) has proposed a new rule that if finalized, would fundamentally change how data brokers are permitted to handle sensitive personal and financial information of consumers. The proposed rule, which uses the Fair Credit Reporting Act (FCRA) as its legal anchor, would classify data brokers who sell sensitive information as "consumer reporting agencies." This specifically means they will be held to stricter standards and real accountability. The following alert outlines the potential implications of this proposed rule and the potential impact on businesses reliant on data brokers, either to verify customers in finance or to tailor marketing efforts.

What Does the Proposed Rule Do?

- **Classification as Consumer Reporting Agencies**: The CFPB's proposal seeks to treat data brokers as consumer reporting agencies when they sell information regarding a consumer's credit history, credit score, debit payments, and income/financial tier. The sale of such information would be considered to be selling a consumer report – regardless of whether the data broker intended the information to be used for the purposes of assessing creditworthiness.

- **Accuracy Requirements**: Data brokers must ensure that the information they peddle is correct. No more wrongful loan denials based on faulty data.

- **Clear Consent**: Data brokers will be required to obtain consumer consent through a written or electronic signature and also provide clear and explicit disclosures before collecting or sharing sensitive information. The proposed rule identifies various requirements for the consent to be valid, including the name of the recipient, the purpose for which the report is being shared, and the name of the consumer reporting agency furnishing the report.

- **Legitimate Uses Only**: Sensitive identifiers (like Social Security numbers) couldn't be sold for marketing purposes. Instead, they'd be reserved for bona fide uses, such as identity verification and fraud prevention.

Who Stands to Benefit?

According to the CFPB, this rule isn't just about raising the industry's ethical bar – it's also about protecting those most at risk. CFPB Director Rohit Chopra has positioned the measure as both a privacy shield and a national security safeguard given the various ways that information obtained from data brokerages can be used:

- **Threats to Domestic Violence Survivors:** When abusers can buy their targets' addresses, the concept of "safe harbor" evaporates. The proposed rule aims to prevent such dangerous disclosures;

- **Risks for Law Enforcement Officers and Judges:** Public servants charged with upholding our laws have found their private lives exposed, increasing the risk of stalking, harassment, and even violence; and

- **Military and National Security Concerns:** Foreign adversaries could purchase personal data to track U.S. military personnel and government officials. This rule aims to slam that door shut before it swings any wider.

What's Next?

The proposed rule comes at a time of uncertainty among lawmakers. The upcoming change in administration could mean a change in priorities and result in the rule being watered down or scrapped altogether. The proposal is facing pushback where industry advocates argue that restricting certain data could hinder legitimate activities like fraud detection or law enforcement investigations.

The proposed rule is currently subject to a three-month comment period, ending on March 3, 2025. However, with many changes in the political landscape on the horizon, the idea of increased regulation in the near term seems unlikely. Nonetheless, businesses reliant on data brokers, whether to verify customers in finance or tailor marketing efforts, should assess how these proposed changes may impact their operations. Firms may need to vet their vendors more thoroughly, adapt compliance protocols, and prepare for the possibility that some data sources might dry up or become more expensive. Commenting on the CFPB's proposal is one way for businesses to shape the final contours of these rules and ensure their voices are heard.

For all its initial force, the CFPB's proposed rule now stands on shifting ground. While the agency's national security framing may grant it a measure of political resilience – at least in theory – the reality is more uncertain. As a new administration takes charge and likely seeks to undo many of the CFPB's recent efforts, many expect the proposal to emerge weaker and heavily revised, if it (or the CFPB) survives at all. Industry advocates are already poised to push back, and the question of whether this kind of data will truly be considered a "consumer report" remains unresolved. In the end, the rule's ultimate form and impact could be far more limited than originally envisioned, though additional regulation affecting data brokers domestically and abroad continues to be likely.

Whether this proposal becomes a landmark in privacy law or a fleeting gesture of regulatory ambition, it signals a broader trend: privacy is no longer a side note, but a central theme in compliance and governance.

If you have any questions or concerns about this topic, please reach out to Alexander F. Koskey, CIPP/US, CIPP/E, PCIP, Matthew G. White, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, Madison "MJ" McMahan, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.