

The Delicate Dance of Data Security in Open Banking

In a recent comment letter, data security in open banking, the Bank Policy Institute (BPI) and The Clearing House (TCH) expressed reservations about the Consumer Financial Protection Bureau's (CFPB) open banking proposal, emphasizing the need for more robust measures to safeguard sensitive consumer financial data.

The proposal aims to grant consumers greater control over their financial information by compelling banks to share data with third-party entities, particularly fintechs. While the CFPB insists on providing personal financial data at no charge through secure digital interfaces, banking trade groups are calling for broader application, covering all third parties and data aggregators.

Banking Associations Advocate Broader Application of CFPB's Proposal

The BPI and TCH assert their support for fostering competition through innovative financial technology but emphasize that it should not compromise data security. They urge that consumers' personal and financial information must remain secure during transactions between financial institutions and third parties, as well as when stored externally.

Screen Scraping Prohibition and Liability Definition Demanded

The CFPB's proposal seeks to move away from the contentious practice of screen scraping, a method labelled as a "risky data collection practice." Screen scraping often involves consumers sharing their usernames and passwords with third parties, raising significant security concerns.

Keep Reading

The banking associations propose a more stringent stance against screen scraping by prohibiting the practice once a data provider offers a developer interface. Additionally, they advocate for direct requirements on authorized third parties and data aggregators, with an explicit commitment from the CFPB to supervise compliance.

Liability remains a key concern for the BPI and TCH, who argue that aggregators and other data recipients should be held accountable for unauthorized transactions or failing to protect consumer data in their

