Banks want liability risk clarified in CFPB open banking rule

By Kate Berry

August 23, 2024, 11:11 a.m. EDT

Bankers are expressing concern that the Consumer Financial Protection Bureau's proposed open banking rule is insufficiently clear about whether banks or third-party service providers will be held liable for data breaches or fraudulent transactions, and fear they will be forced to reimburse consumers for errors that aren't their fault.

As financial institutions gear up to implement the CFPB's open banking rule, which is expected to be finalized in October, banks are trying to get a handle on how to manage third-party risks, a tall task in an ecosystem awash with data and a burgeoning industry of upstarts calling themselves financial technology providers.

The CFPB is expected to finalize its 1033 open banking proposal in October, giving consumers a legal right to grant third parties access to bank data. The bureau's plan — authorized by section 1033 of the Consumer Financial Protection Act of 2010 — will require that banks turn over sensitive data on transactions in checking accounts, prepaid cards, credit cards and digital wallets to competitors.

Some experts think the 1033 rule will empower community banks and fintechs to better compete against large banks and reshape how consumers use their personal financial data. But the

timeframe is narrowing for banks to get their message across about the difficulties of implementing 1033.

"It would be helpful if industry knew what to expect with liability and how it is going to be apportioned, but the proposal doesn't have that," said Brian Fritzsche, vice president and associate general counsel at the Consumer Bankers Association. "It's like hitting a moving target blindfolded."

While the shift to open banking is expected to increase competition for financial products and services, banks are raising alarms about specific problems with the CFPB's proposal that they think needs to be fleshed out in a final rule. Banks claim liability is not addressed with enough specificity to ensure that it is fairly apportioned and generally "follows the data." As the main data providers, banks want the CFPB to allow data providers to deny access to third-parties and data aggregators based on risk management concerns.

"When you have these other parties, is there inter-party liability? If a data aggregator suffers a data breach, should there be some kind of liability to the data provider if a consumer has been harmed?" asked Fritzsche.

Banks do not want to be held responsible for incidents like data breaches that occur after the data has left a bank's control. Banks generally want each entity to be liable for — and be required to indemnify other entities — losses resulting from unauthorized transactions, harm arising from a data breach, or other problems. Assigning apportioned liability would provide an incentive to the third parties to implement and maintain robust data security programs.

Bradley Wallace, compliance director at core processor CSI, said existing regulations make clear that banks are on the hook for overseeing third parties.

"It's been made clear in third party risk management guidance that the financial institution is ultimately responsible for the data, and the only way to mitigate the liability risk is to have robust due diligence," said Wallace. He advises companies to have their boards and top management review the interagency guidance on third-party risk.

On a recent quarterly compliance call with 400 representatives from community banks to discuss the CFPB's final 1033 rule, Wallace said he found "glaring deficiencies" at banks that don't have appropriate risk management processes in place.

Many small community banks have executives who are wearing "lots of different hats," he said, and they need to understand what the market is doing, including "learning the jargon" of 1033. That includes being able to explain to boards how the rule works and how to implement it.

"They should be able to define what an API is to management, business partners within the industry, and then make sure they're putting together a robust risk assessment and a vendor due diligence program to ask the right questions of third parties," Wallace said.

Third-party data sharing is already being widely used for a range of banking activities, including paying bills, sending money, getting a loan, paying taxes and investing. But not all payment methods and systems have the same consumer liability rules or risks. The CFPB's 1033 proposal

envisions that the current liability framework should be similar to regulations implementing the Electronic Fund Transfer Act and the Truth in Lending Act. The bureau also refers in its proposal to bilateral contracts between companies.

But Fritsche said banks want clear liability and indemnification rules to ensure that they do not bear additional risks or costs that may occur when a third-party provider fails to protect or misuses the data after receiving a consumer's instructions.

In addition, banks face more than just a technical challenge in delivering data requested by consumers. The largest banks, which must implement 1033 within six months of a rule becoming final, are currently in the process of building internal systems to automatically fulfill requests for information.

Jim McCarthy, a former CFPB official and chairman of McCarthy-Hatch, a risk and compliance firm, said the bureau already is testing the readiness of banks in providing data to consumers. McCarthy said he has a theory about how the CFPB is using consumer complaints to ensure that banks are responding to data requests.

Earlier this year, the CFPB added two data points to its nonpublic complaint intake form, asking consumers if they requested information from their bank and if they received all of the data in a timely manner.

"They are leveraging the request for information requirements to determine banks' readiness for 1033," McCarthy said. "If they find that banks have no ability to identify and respond to requests for information, it would be an example of the absolutely huge lift that it will take for a bank, especially [the biggest] banks, to implement 1033."

McCarthy, whose firm examines consumer communication with individual banks, said that he has found that each of the top banks have "a massive deficit in responding to requests for information in accordance with the guidance of the rule."

"It is a big problem and it's going to be a big lift," he added.

The massive scope and technological complexity of the rule has led the CFPB to break it down into at least two parts so far. In June, the bureau finalized part of its open banking rule that established criteria to recognize organizations that set technological standards. The bureau has made references in notices and its unified agenda to subsequent rules.

Banks and some data aggregators have asked the CFPB for an extended two-year timeframe to comply with the final rule on personal financial data rights.

So far, though, the CFPB is taking a cascaded approach to implementation. Banks with at least $500 billion in assets and nonbanks with at least $10 billion in assets must comply within six months. Banks with between $50 billion and $500 billion in assets and all other nonbanks have a year to comply. Banks with $850 million to $50 billion in assets have two and a half years, while the smallest depositories have four years to comply.

The timeframe for implementing the rule is also important because banks have asked the CFPB to initiate a larger participant rule that would bring the largest data aggregators under the bureau's supervision.

"Who's going to examine and supervise those entities to be sure they're complying?" asked Fritzsche.

Wallace thinks open banking is an opportunity for community banks to deliver better products and services.

"Community banks now have the ability to compete on par with the big boys that collect data that they have held hostage for many years," Wallace said. "I think community banks will gain far more customers than they will ever lose from open banking which is the door to give them the right technology and information about the consumer."