Open Banking: U.S. Regulators Pressed On Data Security Responsibilities

10TH SEP 2018 | WRITTEN BY: ADAM PERROTTA IN LOS ANGELES

Although U.S. federal authorities have received industry praise for espousing a hands-off approach to open banking, signs are emerging that consumers may prefer lawmakers and regulators to play a stronger role, especially in ensuring their data is protected.

In a wide-ranging report on fintech released in July, the U.S. Treasury touted the benefits of data aggregation and sharing for personal financial services, via methods such as screen scraping and APIs (application programming interfaces).

Although onlookers welcomed Treasury's support for organic growth, a recent survey conducted by The Clearing House found that a significant portion of consumers expect officials to play a much more active role.

When asked which entities they expected to "exercise leadership" in addressing data security and privacy concerns in the context of open banking, 47 percent of respondents cited regulatory agencies, while 33 percent called for direct government or congressional involvement.

Some 35 percent of respondents who used fintech services said they hold governments and regulators directly accountable for the security of their financial data.

One significant issue that could arise from such a discrepancy is that states could then be compelled to create their own data security rules — potentially leading to a confusing and contradictory hodgepodge of local data security laws, according to Eli Rosenberg, an attorney with Baird Holm.

"The concern is that, if issues arise and there is a perceived lack of action on the federal level, states will continue to take action individually without consulting with industry, and you end up with a patchwork of laws and regulations for providers to deal with, as opposed to more uniform regulation," he said.

Several states have already ramped up consumer protections in response to the federal government's apparent backtracking in terms of enforcement under the Trump administration and Republican-held Congress.

> "States like Pennsylvania and New Jersey have created their own 'mini-CFPBs,' and a plethora of other states, including California, have recently enacted new consumer data protection laws," said Eli Rosenberg of Baird Holm.

But beyond the official mandate, financial firms have plenty of incentives to ensure consumers' data is safe when shared across their platforms, especially as public awareness of the importance of data security grows.

In fact, such companies are increasingly viewing the ability to offer robust data security as a competitive differentiator in the battle for market share, noted Lori Breitzke, president of E&S Consulting.

Financial services providers "must continue to consider and address the issue of acquiring and retaining customers," said Breitzke.

"This will necessitate maintaining a high level of data security, because if consumers even sense that their data is not secure, they will move on to the next financial services provider. They have a choice today, and they know it."

Among industry stakeholders in the open banking ecosystem, banks themselves could prove the entities best-suited to acting as gatekeepers, having been consistently ranked as the private entities trusted most by consumers.

In a 2017 survey by A.T. Kearney, more than three in five respondents had confidence that their primary banks could ensure their personal information was protected — easily outpacing other private providers.

Just 21 percent of respondents said financial information aggregators could ensure data security.

In addition to enjoying a high level of consumer trust, banks are in a position to set data security standards for their fintech partners and third-party vendors as a result of being the primary holders of most consumer financial information.

"Something we often see are requirements imposed on banks, with the expectation that the bank will flow those requirements down to any service providers or other third parties it engages," said Rosenberg.

Private stakeholders are often the most effective "enforcers" when it comes to implementing data security measures, Breitzke noted, citing the card network-mandated implementation of EMV technology and PCI DSS-based security standards.

Ultimately, according to Rosenberg, whether the public or private sector takes the lead on data security within open banking, cooperation between the two sides will be essential to ensure consumers can take advantage of new third-party offerings without imperiling their personal and financial information.

"I think it is fair to say that industry would welcome the opportunity to work with lawmakers and regulators on commonsense solutions to data security issues," he predicted. "There are roles for both sides to play on the issue."

Commenting as:

Adam Perrotta

Anonymous

Comment *

Submit comment

Related Content

Insights & Analysis

New York Court Ruling Leaves Payroll Card Sector In Limbo

Japanese Officials Hint At Open API Reforms

Privacy Worries Are Stifling Biometrics, Claim US Officials

Italian Authorities Admit Slow Progress On Innovation

Research & Reports

European Commission Consults on Policy Approach to Fintech Industry

EU: Report on Fintech — Influence of Technology on the Future of the Financial Sector

UK: FCA Releases Business Plan for 2018/2019

Approaching Cyber-Crime and Promoting Innovation

UNITED STATES REFERENCE LIBRARY

US: Money Transmitters

Central Bank

Central Bank Payment System Report

BIS Payment System Report

AML/FIU

AML Mutual Evaluation Report 2016

US State Reports

Resources

News
Videos
Webinars
Whitepapers

Contact Info

United Kingdom
St Clare House, 30 Minories
London
EC3N 1DD
United Kingdom
+44(0)207 921 9980

United States Of America
1725 I Street NW, Suite 300
Washington D.C., WA 20006
United States
+1 202 261 3567