The Negative Consequences of Mandating a 90-Day Reauthentication Requirement

The Financial Data and Technology Association of North America ("FDATA North America") understands that some large U.S. financial institutions, as well as some policymakers, are contemplating the imposition of a mandatory 90-day reauthentication requirement for any credentials or tokens utilized by end customers to access third-party financial tools. While such a requirement is being contemplated with the goal of improving protection of customer data, the experience of the U.K. market, in which 90-day reauthentication is required, proves the opposite. We provide here a high-level overview of the detrimental impact a 90-day reauthentication requirement would have, based upon the experience of a market that is currently struggling underneath such a mandate.

Overview:
Due to the 90-day reauthentication requirement in the U.K., to use third-party provided financial products and services of their choice, customers must reauthenticate each app they utilize, through their bank, every 90 days. Mandating reauthentication events at least once every 90 days harms customers by aggravating their experience and unnecessarily hindering marketplace competition. The goal of an open finance system is to provide customers with control over their own financial data such that they can choose the financial providers they wish. FDATA North America believes that this control is the single best way to ensure good stewardship of that data.

Adverse Impact on Customers
The 90-day reauthentication requirement in the U.K. has been a leading cause of frustrating customer experiences. According to a leading U.K. Open Banking third party provider of critical financial services, the 90-day reauthentication mandate in that market has resulted in customer churn – the percent of customers no longer active on the platform – spiking nearly seven times, from 6.9% prior to implementation of the mandate to 44% afterwards. In addition, though survey data showed that 96% of their customers would be disappointed if they could not use their app, and 80% prefer to manage their money on the third-party app instead of a banking app, nearly half of the customers of one app in the U.K. are not maintaining their relationship and are no longer accessing critical financial tools.

Based on current fintech adoption rates, churn that approaches even a fraction of this level in the U.S. market would equate to millions of U.S. consumers and small businesses abandoning tools that are providing critical access to financial services. Moreover, mandating a time-intensive reauthentication event every three months is not the only way to ensure customers are aware of their third-party connections, even if it may be the most intrusive. Dashboards, periodic reminders to customers as to which third-party apps have their information, and other less invasive tools all provide the same customer empowerment without the negative consequences of loss of connectivity to essential financial services applications.

Reducing friction for customers by ensuring high-quality products and a frictionless user experience is essential for customer retention and, in the context of technology-based tools that facilitate better financial outcomes, imperative towards improved financial access. Introducing artificial friction via a mandatory 90-day reauthentication process forces a frustrating experience upon the customer that can result in them abandoning use of an otherwise helpful tool as their connection to that tool repeatedly breaks. Additionally, some customers may also not realize the benefit of an application they are using until after a period longer than 90 days. Customers may only use certain financial tools actively every six to twelve months but still derive significant value from maintaining data connectivity in those applications, including, for example, cash flow data-underwritten revolving credit, overdraft fee protection applications, or payment platforms.

Additionally, the overwhelming majority of financial technology customers have accounts with multiple institutions. Accordingly, a 90-day reauthentication mandate would require reauthentication with each different institution every 90 days to keep using the service of their choosing. Practically speaking, a customer with, for example five accounts connected to fintech application, would actually be required to reauthenticate, on average, once every 18 days to avoid losing functionality in their chosen application.

Customers have vastly different financial needs and benefit from a competitive marketplace innovating to serve them. If competition is stifled, the only beneficiaries are marketplace incumbents, as competition is snuffed out and customers are forced to turn to incumbent products, even if they are of lesser quality or not sufficient for the customer's needs. An essential way to support high quality products and innovation in the marketplace is by ensuring market competition, customer choice, and driving the need to constantly innovate to provide the best customer experience. In addition, the continuous need for reauthentication prevents certain features from being developed and launched, such as overdraft protection, which can make a critical difference in customer's financial lives.