PaymentsCompliance

Published on *PaymentsCompliance* (https://paymentscompliance.com)

Regulators Look To Wield Open Banking Against Financial Crime

22ND OCT 2019 | WRITTEN BY: DOUGLAS CLARKE-WILLIAMS

Regulators have mooted the possibility of beating the ploughshare of open banking into a sword against financial crime, but technical and legal hurdles still stand in the way of authorities' ambitions.

Application programming interfaces (APIs) are central to open banking, and until now attention has largely been focused on their role as a gateway by which third-party fintechs can access consumer accounts at financial institutions.

But some regulators have been looking beyond commercial uses and considering how national competent authorities (NCAs) might employ APIs in their own ongoing efforts to tackle financial crime and ensure compliance by regulated entities.

Christopher Woolard, executive director of strategy and competition at the UK's Financial Conduct Authority (FCA), suggested recently that "APIs developed by firms to share information in a structured manner under open banking could also be used to transport and share fraud data in the UK".

Rūta Merkevičiūtė, head of the payments and e-money division at the Bank of Lithuania, foresaw an even wider horizon of possibilities for supervisory APIs.

She suggested that the regulator could use account information services to view the safeguarding accounts of e-money firms, ensuring at a glance that the companies are holding the required amount of capital and that the transactions associated with it all abide by the relevant requirements.

"To see how much is kept, if it's kept properly, we think perhaps account information services will be useful in our hands," she said at the Open Banking Expo in Amsterdam earlier this month.

Speaking to PaymentsCompliance on the sidelines of that conference, Merkevičiūtė floated an even more extensive use of APIs by the regulator, saying that the central bank was looking into using them in the fight against financial crime.

"We think maybe we could connect to the entities and take their transactional data, and form the reporting from that data," she said, suggesting that by taking such data directly the regulator would bypass the bank's need to assess and package the data itself and avoid miscommunication between the authority and those it oversees.

The Baltic state's project has already shifted into a procurement phase. The central bank has two companies pitching "to develop how they could bring from transactional data statistical reporting or anti-money laundering (AML) reporting".

Although regulators may be eager to bring new technology to bear upon old problems, a number of legal and technical issues could get in the way.

Foremost among these are data privacy concerns. Potential clashes between the revised Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR) were a legal hydra in the early days of the former, and the kind of overview envisaged by Merkevičiūtė has the potential to cause similar issues.

"There would be data privacy concerns, and implications to such access by the regulators from a GDPR standpoint," said Yulia Makarova, of counsel at Morrison & Foerster.

"If the regulators were to monitor certain operations or fund flows, or banks' general compliance with the regulations, they would inevitably need access to information about specific transactions and that will bring it into GDPR territory."

Such data protection concerns would not only be between the bank or payment provider in question and the regulator, but could also see the NCAs' responsibilities greatly expanded once they come into possession of individuals' transaction information.

Douglas Mathie, of counsel at CMS, said that "if a regulator starts taking data, effectively copying it from a bank's system to a regulator's system, then the regulator will probably become a data controller in terms of data protection law".

Such a shift "would come with its own issues for the regulator, including data protection duties to the end customer", he said.

A further issue is that financial institutions owe a duty of confidentiality to their customers, and cannot disclose personal or account details without explicit consent — a mechanism which is built into an individual's approval of a third-party provider's access to their account in the course of commercial open banking.

No such mechanism as yet exists for a consumer to allow a regulator consistent access to their financial data.

Although banks are obliged to give up transaction data to NCAs if required, this usually occurs in the process of enforcement investigations.

"These powers are quite specific and are subject to certain conditions being satisfied and criteria being met for the regulator to have authority to commence the investigation," Makarova said.

"If we're talking about the regulators gaining access to APIs and therefore to confidential information for the purposes of oversight, my take on it is that there should be further changes to the regulations to expressly allow the regulator to do that."

Mathie, however, suggested that the consistent underlying principle of banks being "compelled" to give up data to NCAs when required could be expanded to the kind of API oversight mooted by Woolard and Merkevičiūtė.

"All they're really doing here would be automating that process through an API or an interface, so I don't think there's a big difference in what's being done, why it's being done, and the legal justification for it," he said.

Should such issues be settled, it would still remain for the actual infrastructure to be built.

Merkevičiūtė declined to say which companies were currently involved in this initial proof of concept stage, but they would face a challenge in effectively centralising a system which at present is handled by banks assessing their own transactions and then submitting the required reports to the regulator.

Paolo Spadafora, chief executive of digital banking platform Epiphany, noted that regulators would need a "big budget" to effectively monitor transactions through APIs.

"The first thing to consider is that volumes represent a big issue, as it is impossible to look at billions and billions of transactions: there is the need to set a filter given the large-scale dimension of the architecture, and most of the time it is difficult to allocate resources to do this," he said.

He suggested that the most effective model would see a measure of the work continue to be carried out at the bank level, with a component owned by the regulator "deployed within the bank infrastructure" which would perform the necessary filtering.

Spadafora estimated that this would still take "a couple of years" to be implemented across the sector, and would also still require auditing by the authority to ensure the technology was being correctly and consistently used.

He did note that supervision of safeguarding accounts through APIs would be easier, "because it is just needed to interface with the treasury system. It will be a new API they have to expose, and it's simple to understand if they have the money they should have to offer a safe environment for their customers."

There is currently no set timeline for the Lithuanian initiative. Merkevičiūtė indicated that the central bank would be able to assess the viability of any prototype in six months.

TOPICS

Filter: Data Protection

Filter: Financial Crime

Filter: Payments Regulation

Consumer Protection

Data Protection

Personal Data

AML/KYC

Financial Regulation

Open Banking

GEOGRAPHY

Lithuania

United Kingdom

Europe

SECTORS

Banking

Fintech

Third-Party Providers

CONTENT

Insights & Analysis