LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Fintech Faces New Compliance And Enforcement Challenges

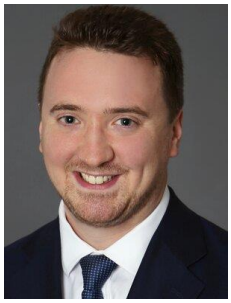
By **Sara George and Max Savoie** (August 11, 2022, 1:57 PM BST)

Sara George

The payments and crypto-assets sectors are a focal point for regulatory actions to prevent financial crime, particularly fraud and money laundering.

Many firms operating in these sectors in the EU and U.K. are already subject to detailed regulatory requirements, and those are likely to be broadened over the coming years.

Parts of the payments sector are also systemically important and the potential impact upon financial stability of their failure means that this aspect will continue to be at the forefront of regulatory priorities for the foreseeable future.



Max Savoie

There is a growing perception among regulators and policymakers that the sector has previously been too lightly regulated and, as a result, insufficient attention was given to the protection of consumers, the safeguarding of funds, the implementation of adequate anti-money laundering and financial crime controls, and the independence, fitness and propriety of owners and controllers.

Firms often need to make difficult trade-offs between user experience, risk management and data privacy.

This article discusses how regulation and supervisory actions by regulators are affecting those trade-offs.

What Are the Key Financial Crime Risks Facing Payments and Crypto-Assets Firms?

Payment service providers and the crypto-assets sector are especially vulnerable to their services being used for the facilitation of financial crime.

These may include the defrauding of consumers through authorized push payment fraud to enabling offenses, such as allowing the sums extorted by cybercriminals involved in ransomware attacks to be moved beyond the jurisdiction of the courts, financial sanctions circumvention and the laundering of the proceeds of other criminality.

What Are the Rules, and How Are They Changing?

Payment service providers, such as banks, electronic money institutions and payment institutions, are subject to a relatively prescriptive set of standards relating to data security and fraud prevention under the framework established by the revised EU Payment Services Directive, known as PSD2.

These include requirements relating to strong customer authentication, secure communications and fraud reporting. Payment service providers are also generally subject to anti-money laundering requirements, including risk-based customer due diligence and suspicious activity reporting under the revised EU Money Laundering Directive, or MLD.

The U.K. has broadly continued to apply requirements under the PSD2 and MLD regimes since it left the EU.

The European Commission is currently reviewing PSD2 and is likely to publish proposed changes later in 2022 or early in 2023.

In particular, it is considering whether to expand the scope of PSD2 to a broader range of providers, including technical service providers that are currently excluded from the regime.

This reflects a broader shift by regulatory policymakers toward direct regulation of technology and fintech firms that support the provision of financial services. Such firms can play an important role in measures to prevent financial crime.

There is no guarantee that the U.K. will implement equivalent changes. Rather, regulatory policymakers in the U.K. may be feeling political pressure to demonstrate that they are using their post-Brexit discretion to plot a different course.

However, financial crime prevention, including fraud prevention and anti-money laundering continue to be a focus of the U.K. Financial Conduct Authority and the U.K. Payment Systems Regulator.

On this basis, while we may see divergence in some of the more detailed technical standards, where the U.K. may take a more principle-based approach to regulation, the overall direction of travel is likely to be toward increasingly robust and broad-reaching regulation.

Crypto-assets, on the other hand, may have greater potential to trigger regulatory divergence between the EU and U.K. Both the EU and U.K. have extended requirements under the MLD regime to apply to certain crypto-asset exchange and custodial wallet providers.

However, the U.K. has taken a broader approach by including providers of crypto-to-crypto exchange services and issuers of crypto-assets within the scope of such requirements.

The U.K. is also taking a more iterative approach in its plans to expand regulatory authorization, prudential and conduct of business requirements to the crypto-assets sector.

While the EU is pressing ahead with its proposed Markets in Crypto Assets Regulation,[1] which will bring a broad range of crypto-assets within scope of such requirements, the U.K. is — for the time being at least — focusing on narrower plans to regulate fiat-currency-linked stable tokens, as well as the marketing and promotion of crypto-assets more generally.

Another key reform for which crypto-assets businesses in the EU and U.K. need to prepare is the

extension of funds transfer regulations to certain transfers of crypto-assets.

These regulations currently apply only to certain transfers of fiat currency and require payment service providers to include information relating the payer and payee together with the funds transfer to ensure the transaction can be traced back to them.

Applying these requirements to crypto-asset transfers may help to mitigate against certain of the perceived financial crime risks associated with crypto-assets. However, implementing such requirements could pose significant operational challenges for the sector.

What Are the Key Regulatory Enforcement Risks for Firms?

Unsurprisingly, as a result of the experience of the first failures of nonbank payment service providers, new entrants to the market are subject to far greater scrutiny of their willingness to observe the requirements of a principles-based regulatory regime, which relies upon firms making voluntary disclosures to their regulator against their interests and being cooperative partners in achieving good outcomes for consumers and in maintaining the integrity of financial markets.

It is far easier for a regulator to take preventive action by refusing to authorize a service provider where it has doubts as to its ability to regulate the provider effectively, than it is to bring enforcement action when that provider fails to meet the required standards.

We should therefore expect to see more detailed analysis of applications and robust challenges to assertions made in support of the applications, especially where they relate to structural issues that have the ability to compromise other market participants, prejudice consumers or facilitate serious or organized crime.

The Financial Conduct Authority has pioneered the use of innovative civil remedies in the regulatory context, such as injunctions and restraining orders, where there is an immediate risk of harm as an alternative to bringing enforcement proceedings.

It prefers expedition and the more extensive powers of the civil courts to hold a noncooperating party in contempt, and to impose sentences of immediate imprisonment on defaulters to the more limited powers of the Upper Tribunal.

While the tribunal can impose substantial financial penalties, it can only do so after a lengthy administrative process, by which time the assets are likely to have been dissipated and no longer available to pay redress to affected parties.

The Big Trade-Off: User Experience, Risk Management and Data Privacy

Payments and crypto-assets firms face a common challenge whenever they bring a new product to market — how to strike the right balance between creating a seamless user experience or the customer journey, while also ensuring preventative measures against financial crime.

Although there is no single answer to this question, it is apparent that regulators are increasingly taking issue with the approaches some firms are adopting. This is particularly the case with customer onboarding where trim know-your-customer processes and failure to oversee and scrutinize third-party service providers can create significant financial crime and regulatory enforcement risks.

Senior management within firms would also do well to remember that regulators expect them to be fully engaged in decisions relating to compliance and financial crime risks and that improvements to the customer experience are virtually never a defense for noncompliance.

Data privacy is another part of the trade-off. Anti-fraud and anti-money laundering procedures often involve processing personal data. Some of the more innovative anti-fraud measures employed in the payments sector involve behavioral and biometric data.

For example, metrics like walking style, typing speed and even your heart rate can be good indicators of whether it is really that individual using a mobile payments app, rather than someone pretending to be that person.

However, the processing of such data also creates risks for the data subject if it were to fall into the wrong hands and raises the question whether the privacy implications are proportionate to the anti-fraud risks for which the data are collected.

Consumers are less likely to be willing to accept the use and potential misuse of their personal data in fraud controls when it is being used solely to protect the payment services provider from losses, but where they have no equivalent exposure.

Acceptance of the implementation of the more intrusive surveillance mechanisms that are now possible is reliant upon the sector persuading the public that the malignancy and prevalence of financial crime and its corruption of civil society is such that it is proportionate to allow intrusive surveillance mechanisms to be implemented collectively, with individuals deemed to have consented in the wider public interest.

Ultimately the parameters around such trade-offs are a matter of public policy and will be determined by legislators and regulators.

Firms should therefore ensure they understand their regulatory obligations and take account of the risk of regulatory enforcement action when considering more aggressive options.

They should also continue to scan the horizon for regulatory reforms in this area, as these can shift the balance of opportunity and risk in such decisions at a fundamental level.

Sara George and Max Savoie are partners at Sidley Austin LLP.

[1] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.