PAYMENT REGULATIONS

Protect and Detect

Staying Ahead of Payments Regulations, Sanctions, and Fraud

David Malley
Product Development & Innovation, Payments Centre of Excellence, NatWest

Avani Patel
Head of Commercial Banking, Fraud Management, NatWest

Andy MacDonald
Head of Financial Crime Services, NatWest.

Regulators are busy laying the groundwork for wholesale payments to become faster, cheaper, and more transparent. With the roll-out of ISO 20022, PSD3 on the horizon, SEPA Instant Payments becoming mandatory, and the UK's New Payments Architecture replacing Faster Payments and eventually BACS, European treasury teams are facing significant change. Meanwhile, corporate sanctions management remains in one of its most complex phases from the past decade. And fraud prevention continues to be a critical concern, as fraudsters evolve at least as quickly as the safeguards developed to keep them out. Here, three specialists from NatWest examine the essential payments developments for treasury teams to prepare for.

Nothing is certain but death and taxes – or so the saying goes. But regulation could arguably be added to the list, especially in the world of payments. As innovation continues to hot up, with everything from variable recurring payments to CBDCs in the spotlight, regulators are working hard to ensure the framework around payments matches the pace and direction in which the industry is travelling. And always with an eye on balancing consumer and business protection against commercial needs, economic drivers, and competitive innovations.

But payments regulation isn't always a case of playing catch-up with tech and behavioural trends. In fact, PSD2 (and the corresponding UK Payment Services Regulations – PSRs) was the catalyst for arguably one of the most significant shifts in the payments arena in recent times – open banking. Today, discussions are happening around PSD3, and the latest developments will inevitably impact corporate treasury teams.

David Malley, Product Development & Innovation, Payments Centre of Excellence, NatWest, outlines: "In May 2022 the European Commission [EC] issued a public consultation to gather evidence for its review of PSD2. Then, in February 2023, the EC presented a study on the application and impact of PSD2. This outlines whether the objectives of the original directive have been met and explores what improvements should be made in the next iteration. And in the UK, HM Treasury has been asking similar questions through its 'Call for Evidence' on the PSRs."

> *"SCA has helped to reduce fraud losses and even eliminate certain forms of attack, but threats keep evolving."*

Then, in late June, the European Commission published its legislative proposal for PSD3[1], it does give a clear indication of the direction of travel. According to Malley, the key areas of focus relevant to corporate treasury teams are:

1. Open banking and the transition to open finance
2. Strong customer authentication requirements – and striking the right balance
3. Combatting fraud more effectively

Open banking turns up a level

The open banking story is often cited as a slow burn, certainly in mainland Europe. After several years of usage, 2021 stats showed that less than 5%[2] of consumers in the EU were leveraging open banking. But the UK surpassed seven million[3] users for the first time in January 2023, indicating an ongoing growth trend (see box 1).

Malley believes that EU adoption could be increased much further, and more rapidly, with the simplification that PSD3 promises. He explains: "There is broad recognition that the PSD2 provisions on access to accounts were effective in opening up the market, doing what was always intended in terms of authorised third-party access to information or payment initiation."

BOX 1 | UK PROGRESS ON OPEN BANKING

In the UK, open banking is evolving and in April 2023, the Joint Regulatory Oversight Committee (JROC) published its recommendations for the next phase of open banking in the UK.

The JROC's recommendations contain a roadmap of priorities over the next two years, covering five key themes :

- Levelling up availability and performance
- Mitigating the risks of financial crime
- Ensuring effective consumer protection if something goes wrong
- Improving information flows to third-party providers (TPPs) and end users
- Promoting additional services, using non-sweeping VRPs as a pilot

While the UK's approach deviates somewhat from that of the EU, Malley believes that the two paths will converge and work in tandem to promote the future of open banking and open finance.

But, without doubt, open banking can be improved and expanded, he believes. "Some of the open banking requirements under PSD2 are contradictory, particularly where they interface with strong customer authentication [SCA]. There is some welcome clarification under PSD3 and we hope that any future changes to the UK PSRs will simplify the regimen."

Elsewhere, Malley also sees a need for the development of more standards around APIs, which are one of the core technologies underpinning open banking. In fact, APIs already enable users to easily trigger single payments and create mandates for variable recurring payments (VRPs). Open APIs have also already empowered A2A payments by removing the barriers of fragmented legacy rails and introducing pay-by-bank capabilities. And as open banking evolves into open finance, enabling a much broader range of data to be shared and creating opportunities for more tailored financial offerings[4], more APIs will enter the mix, hence the growing need for standardisation.

Although the final text, and indeed timeline of PSD3 is still to be determined, corporate treasurers should benefit from the clarification, evolution, and standardisation that is anticipated around open banking. Malley elaborates: "In terms of collecting payments, improvements to open banking will ensure that PISP [payment initiation service provider] payments are truly competitive. This should then give treasurers some leverage in their negotiations with card providers, for example. More innovative financial solutions should also be able to be plugged directly into bank and corporate systems, thanks to standardised APIs."

Improving strong customer authentication

The second pillar likely to be addressed under PSD3, SCA (see box 2 for a refresher), also faces some current challenges, despite its effectiveness.

Malley comments: "In both the UK and EU, many market participants would likely say that the SCA requirements, while well-intentioned, are probably over-prescriptive by insisting on two-factor authentication."

David Malley
Product Development & Innovation, Payments Centre of Excellence, NatWest

Indeed, Malley believes that "SCA can even be considered counterproductive in some situations, especially when we have new tools to predict and prevent fraud, with a focus on risk analysis. The hope is that future developments will place more of an emphasis on outcomes rather than prescriptive factors".

Avani Patel, Head of Commercial Banking, Fraud Management, NatWest, adds that: "SCA has helped to reduce fraud losses and even eliminate certain forms of attack, but threats keep evolving and the key challenge is to find an optimum balance between the security of the journey and the user experience as PSD3 progresses."

Fraud prevention

The third pillar Malley sees as being critical to PSD3 and the PSRs' review is fraud – with a focus on making electronic payments safer. He says: "There are various ways to achieve this, but in the UK, HM Treasury is certainly looking at slowing down certain high-risk consumer payments as a means to introduce 'good' friction and enable thorough checking. Of course, we support good friction, but it has to be sparingly used."

Fraud prevention is a particular focus for regulators given the rise of authorised push payment (APP) scams, linked to the rise of real-time payments – which are irrevocable – and evolving technology, says Patel. She comments: "APP scams happen when a person or business is tricked into sending money to a fraudster posing as a genuine payee. The criminal might pretend to be from the payer's bank, a government entity, a utility company, or housing conveyancer, for example. Often there is a time-sensitive element to the request, and the fraudster will say that money needs to be moved ASAP, putting pressure on the payer."

In the UK alone in 2022 there were 207,372 incidents of APP fraud with gross losses of £485.2m[5].

"Among the tools and services UK banks offer to help fight APP fraud and reduce misdirected payments are confirmation of payee [CoP] and request to pay," says Patel. "As David mentioned, it is also about introducing 'good' friction into the payment process in order to allow time to determine that a payment is 'right' – and we are likely to see more focus from regulators on this in the future."

Avani Patel
Head of Commercial Banking, Fraud Management, NatWest

All hail ISO 20022

Alongside PSD3 and the reviewed PSRs, one initiative that will help to reduce fraud through the standardisation of payments and the proliferation of rich data is ISO 20022 XML. Malley comments: "As all treasurers will know by now, SWIFT's ISO 20022 migration will drive better quality of outgoing messaging and ultimately improve cross-border payments and reporting."

Although the majority of ISO 20022 work and benefits will fall on financial institutions, corporates will ultimately benefit from enriched data, believes Malley. "With improved data, as well as tracking and tracing capabilities, corporates may find themselves able to more accurately project inbound and outbound flows, in turn helping to optimise working capital. Structured remittance data should also lead to improved reconciliation and enable further automation in workflows. These are just two examples, but more use cases will become evident as the ISO migration takes hold."

NPA and ISO

It is no surprise, then, that one of the tenets of the UK's New Payments Architecture (NPA) is to adopt ISO 20022 as soon

BOX 2 | WHAT ARE THE SCA REQUIREMENTS TODAY?

Introduced under PSD2, SCA looks to enhance the security of electronic payments and protect consumers from fraud. It requires the use of two or more independent authentication factors from the following categories:

1. Knowledge: Something only the user knows, such as a password, PIN, or the answer to a security question
2. Possession: Something only the user possesses, such as a mobile device, smart card, or hardware token
3. Inherence: Something inherent to the user, such as a fingerprint, iris scan, or facial recognition

Already, SCA has proven highly effective. The value of card-not-present fraud declined by 12% in 2021 in light of the market-wide implementation of SCA. In addition, card-present fraud in the form of using counterfeit cards at shops and ATMs declined by 37% in 2020 and by 42% in 2021, thanks to industry standards like SCA.

BOX 3 | FRAUD AND THE TREASURER: THREATS AND RISK MANAGEMENT

Under the umbrella of APP scams, Patel says that businesses continue to face significant threats from social engineering attacks, including CEO impersonation. "Invoice redirection scams also remain extremely common. These happen when a fraudster tricks the business into changing the bank details for payment on an invoice. Criminals target companies by posing as suppliers, or banks, government entities, police and more."

Moreover, invoice redirection can also result from customers' suppliers or advisers' email systems being compromised. "So, all of a sudden, our customer is paying to somebody else because their service provider or their lawyer, let's say, has been compromised. In other words, the fraud is not always committed directly. It could be attached to our customer, but it could originate from our customer's customer or service provider."

Proper payments controls, checks, and balances, are therefore vital – as is a culture of being able to question instructions from anyone inside or outside the company. Vetting third parties heavily before entering into business arrangements, and throughout the relationship, is also important.

Elsewhere, cyber-attacks continue to be a significant threat. Findings from the Cyber Security Breaches Survey 2022 showed that 39% of UK businesses had identified cyber breaches or attacks in the previous 12 months . "Ransomware attacks are among the most common threats from a corporate perspective. This is a type of malware that prevents the user from accessing their computer (or the data that is stored on it) and may spread to the wider business network. The data might then be stolen, deleted or encrypted – even if the demanded ransom is paid."

To help tackle the ransomware threat, Patel believes it is critical for corporates to have an insurance plan in place. And to check what that covers – right down to the fine print.

With more people working from home, another type of fraud that Patel's team has seen a resurgence in, is telephone and screen-sharing scams. "The customer receives a call from a fraudster claiming to be, again, from a trusted organisation like the bank or the police. And of course, the fraudster stresses the urgency of the situation, and then gains access to the customer's computer or email using screen sharing.

"We see this quite often in relation to large payments that are going out to suppliers on a regular basis and the fraudster catches on to the pattern. And from the bank's perspective, it can be hard to recognise as the money is going to a recipient that the customer already pays. So once again, proper controls on the corporate side are indispensable."

Given the cost-of-living crisis, Patel says it's also important to consider the rise in insider fraud "because individuals have increased financial pressures". And as the 2022 Cost of Insider Threats: Global Report reveals, insider-threat incidents have risen 44% over the past two years, with costs per incident up more than one-third to $15.38m .

With this level of internal threat, "it is really important for treasury and wider finance teams to assess what other controls they can put into systems, especially when employees are working remotely," suggests Patel. "It's also key to set security by design when implementing new or updated technology systems, with treasury working hand in hand with IT. What's more, security and fraud prevention measures need to be regularly reviewed since attack vectors are continually evolving."

Fraud fighting resources

Whether based in the UK or elsewhere, there are some good fraud resources available from UK institutions. Patel highlights the following as being of interest to treasury teams:

- A firm's guide to countering financial crime risks (FCG) from the UK FCA
- The National Cyber Security Centre, which has advice for both small and large businesses
- The National Institute of Security and Technology's Cybersecurity Framework

as possible – as a means of keeping the UK at the forefront of payments innovation. The NPA will replace the existing UK Faster Payments scheme and lays out the framework for a replacement to the BACS scheme, in time. And in April 2023, the NPA certification-testing window opened for all interested financial institutions.

Malley adds: "It's now expected that NPA will replace Faster Payments in 2026. And Pay.UK is targeting 2028 for the BACS replacement." In the meantime, there will be a consultation later this year on how BACS should move across to NPA. "This is something I urge corporate treasurers and their payables departments to look out for because it could be quite a significant change – certainly beneficial but it needs to happen in a measured way that corporates are prepared for."

At the same time, the UK has been looking to build more innovative elements into its real-time gross settlement (RTGS) engine. The UK RTGS Roadmap 2024, issued by the Bank of England (BoE) in February 2023, will see the service gradually extending its hours of operation, in a phased approach, perhaps ultimately moving to 24/7 says Malley – although this will present many challenges and is a long way off.

"The roadmap also outlines plans for a new channel to send and receive payments alongside the SWIFT network. This includes considerations about providing a common contingency messaging channel – a solution available to all participants, including a protocol and an infrastructure for data transfer."

In addition, the consultation also outlined a new approach to CBDCs and the wholesale market, which the BoE sees as being fulfilled through the RTGS, says Malley. "There is more focus on a retail CBDC at present in the UK. But the wholesale element is also important. And the key is how you can synchronise settlement so that the payment and asset exchange happen simultaneously."

Meanwhile, in Europe, the European Commission published proposals for the regulation of a digital euro in June. And there is more progress being made in the wholesale CBDC conversation in mainland Europe than the UK, with pilots happening in

BOX 4 | SPOTLIGHT ON SANCTIONS SCREENING

"Effective sanctions screening is vital for corporate treasurers at a time when geopolitical events and outdated systems in parts of the banking sector have increased the risks of operating internationally," says Andy MacDonald, Head of Financial Crime Services, NatWest.

"The events of the Russian invasion of Ukraine last year had a huge impact on the payment-filtering industry with the introduction of significant sanctions. What this means is that, as a treasurer, you can have a thorough understanding of what your business is doing strategically and how that will impact payment flows, but you can't always predict what's going to happen externally."

As a payments processor, NatWest, like its banking peers, noticed that the number of alerts for sanctions went up as Russian sanctions were imposed. "There are things we, as a bank, can do to assist here, like training staff across all types of alerts and ensuring they are nimble enough to move to where the support is needed.

"But on an industry-wide level, the utility concept is gaining traction. This is where the transaction filtering is not done by a bank necessarily. Instead, it is performed by a separate entity – a utility that sits outside of a traditional banking network." There are currently a few utilities in existence, says MacDonald, although it is a nascent industry. "The eventual idea is that multiple banks will send their transactions through those utilities, which will provide level screening for sanctions, thereby enabling greater standardisation."

There are additional advantages to the approach, he believes. "For example, it is likely to lower the cost for banks in terms of filtering transactions and this will filter through as financial benefits for consumers and corporates."

Nevertheless, the accountability to ensure that payments that breach sanctions are not made still sits with the banks. "As such, banks will need to ensure that they have appropriate oversight and that there is a backstop if something doesn't go as planned." This is especially important given that the same sanctions lists might be implemented under different regulations in different countries. "So, for example, a number of different sanctioning bodies (including the EU and individual countries) align to the UN sanctions list, but the dates at which the regulatory lists are updated may vary. This can lead to unexpected exposures, which need to be carefully managed."

In terms of oversight, MacDonald also believes it is incumbent upon every party to a financial transaction to ensure they understand the specifics of the sanctions regulations because they can vary significantly as to whether the transaction is to be blocked or rejected. "And resolving any issues can happen much more quickly if everyone, including the treasurer, is up to speed on the regulations," he notes.

France and Switzerland, for example. Malley believes this could have potential impacts for treasurers in terms of the future of payments (see section 6 of this report/this associated article for more detail on CBDCs and how treasurers can prepare).

SEPA Instant becomes mandatory

Just as the UK is revisiting its instant payment mechanisms and engines, Europe is also revising its real-time payments landscape. "The European Commission has mandated that instant payments in euro must be available to all citizens and businesses holding a bank account in the EU and in EEA countries," says Malley.

Andy MacDonald
Head of Financial Crime Services, NatWest.

> *"Effective sanctions screening is vital for corporate treasurers at a time when geopolitical events and outdated systems in parts of the banking sector have increased the risks of operating internationally."*

The proposal, which amends and modernises the 2012 regulation on the Single Euro Payments Area (SEPA), aims to ensure that instant payments in euro are affordable, secure, and processed without hindrance across the EU. This will rely on increasing trust in instant euro payments, with an obligation on providers to verify the match between the bank account number (IBAN) and the name of the beneficiary provided by the payer in order to alert the payer of a possible mistake or fraud before the payment is made[6].

In addition, the proposal requires the removal of friction in the processing of instant euro payments, while preserving the effectiveness of screening of persons that are subject to EU sanctions (see box for the latest insight on sanctions screening), through a procedure whereby payment service providers (PSPs) will verify their clients against EU sanctions lists at least daily, instead of screening all transactions one by one[7].

According to Malley, it is likely to be the end of 2024 before sending and receiving instant euro payments is mandatory for EU PSPs in the Eurozone (who offer their customers the sending and receiving of euro credit transfers) and the end of 2026 before they also become mandatory for EU PSPs outside the Eurozone. "While there is significant work to be done to implement the changes, we believe the shift from next-day transfers to transactions being completed 'within ten seconds' will be broadly beneficial for all involved, including treasury teams," he observes.

Embracing the change

Summarising the shifts in the regulatory, fraud, and sanctions landscapes, Malley comments: "Change is the way of the world. Treasurers can no longer afford to live in the past or only look at what's happening in the present. The future is being shaped today, and there are significant cash and risk management benefits to be had by being part of those conversations early on and seizing the opportunities on offer."

Notes

1 Please note: the June proposals actually include several elements. Much of what was in PSD2 is proposed to be in a new Payments Services Regulation, while the Payment Services Directive itself focuses on authorisation of firms including for electronic money. In this article we refer to PSD3 for convenience. The legislative process still has a way to go.
2 https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_1819
3 https://www.openbanking.org.uk/news/uk-reaches-7-million-open-banking-users-milestone/
4 https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_1819
5 https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app
6 https://ireland.representation.ec.europa.eu/news-and-events/news/european-commission-proposes-accelerate-rollout-instant-payments-euro-2022-10-26_en
7 https://ireland.representation.ec.europa.eu/news-and-events/news/european-commission-proposes-accelerate-rollout-instant-payments-euro-2022-10-26_en