The
FUTURE SERIES
2022

THE FUTURE OF PAYMENTS 2022

THE CUTTING EDGE OF DIGITAL PAYMENTS

Finextra

BANKING CIRCLE

CBI

FORM3

GOCARDLESS

Infosys | Finacle

THE FUTURE OF PAYMENTS 2022

THE CUTTING EDGE OF DIGITAL PAYMENTS

Finextra Research
77 Shaftesbury Avenue
London,
W1D 5DU
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com

CONTENTS

01 INTRODUCTION

The Covid-19 pandemic and Russia's invasion of Ukraine in 2022 has proven that the financial services industry must be always at the cutting edge of payments.

Amid uncertain times, resilience is key and with the rising cost of living expected in the UK and across Europe, criminals will view this as an opportunity to infiltrate financial systems and attack.

We will need to adapt at the same rate as fraudsters, and all digital systems must be designed with security at the forefront.

Alongside this, education will be crucial to ensuring customers are aware of the risks involved with new financial or payments schemes.

As seen with the UST crash and instability around digital assets, the sector must remain cautious before placing all our bets on uncharted waters.

With expert views from Banking Circle, CBI, Form3, GoCardless and Infosys Finacle, in this report, you will learn from industry leaders about the events and trends defining global payments in 2022 and beyond. The report includes insights from Fluency, Hogan Lovells, IBM, McDermott, Will & Emery, Nationwide, Nordea, Linklaters, TSB Bank and Visa.

02

INSTANT PAYMENTS AND REQUEST TO PAY – ON THEIR WAY TO MAINSTREAM

AN EXPERT VIEW FROM INFOSYS FINACLE

Peter Ryan, Senior Product Manager, Infosys Finacle

Instant payments and its most important application, request to pay is set to revolutionise the payments space and the way we conduct business.

Request to pay is, in fact, already live in the UK (using open banking) and is being rolled out across the Eurozone (using XML messages). It is the ability to make a request for payment electronically. On receipt of the request to pay message, the payer can respond by paying in full, declining payment, making a partial payment, or entering a dialogue with the payee who sent the request for payment.

By linking invoices to request to pay messages efficiency savings can be made in areas such as reconciliation of issued invoice against settling payment and the ability for small businesses to analyse the speed of payment from their customers. However, it is when requests for payment are combined with instant payments that new business opportunities open-up, and many existing processes are streamlined.

Combining instant with request to pay

Take the example of a corporate business that is approaching its credit limit. Rather than doing nothing a bank can send a request for payment message to the corporate customer. If they respond with an instant payment, then this can avoid them exceeding their credit limit and having payments rejected as a result. This safeguards the reputational damage of the corporate customer and provides a better customer experience. Similarly, a rejected Direct Debit could trigger sending a request for payment which would allow the customer to make an instant payment to cover the shortfall if they had funds available in another account.

However, where instant payments combined with request to pay is most likely to become mainstream is the ability to make a payment based on a triggering action such as a delivery of goods or use of a service.

However, where instant payments combined with request to pay is most likely to become mainstream is the ability to make a payment based on a triggering action such as a delivery of goods or use of a service.

Take the example of a pizza delivery. When an order for pizza is placed it has either to be paid upfront by credit or debit card (which runs the risk of non-delivery) or to be paid by cash on arrival. This process can be improved by combining request to pay and instant payments. When the order is placed a request for payment can be made. When the pizza delivery arrives at its destination, the customer can make an instant payment in response to the request for payment. As the request to pay message is linked to the order the deliverer can be alerted (by text or app) that payment has been made and the pizza can be handed over. Obviously, the customer does not have to wait for the pizza to arrive to make the payment, they can make the payment immediately, but if they want the extra safeguard, request to pay provides that.

On a larger scale, this request to pay model can be used for any delivery versus payment scenario: be it a delivery of flat packed furniture at a home, a container at a warehouse or a ship at a port. The use of instant payments in these scenarios gives payment certainty to the business making the delivery, so the process or delivery and payment is simultaneous.

The added value

The added value of request to pay in such a scenario is that the message can be accompanied by an electronic invoice which records what the payment was for. Not only does this provide instant reconciliation but also allows any returns of refunds to be managed electronically rather than customers hunting for paperwork.

The business models discussed so far are dependent on the payer pushing a button to make a payment. Looking to the future, request to pay could be linked with the internet of things. For example, when a car is parked, the car parking can be paid for electronically (by linking a number plate to an account for example). This can be triggered automatically but obviously there is some nervousness with payments being automatically being debited from an account. At the same time, this sort of technology provides a better service than fumbling for coins in the rain to put into a parking meter. Request to pay provides an added layer of security to the process. If instead of automatically debiting the payment for parking a request for payment was sent, then the driver could verify the amount before making an electronic payment.

Request to pay could give customers control over the internet of things by allowing them to control which requests to pay automatically and which request need approval from the account holder. By providing the opportunity of a one-click lifestyle request to pay and instant payments hold the promise of going mainstream and becoming part of our everyday lives.

The next step of course would be the option of automatically fully paying requests for payment from certain pre-validated businesses. For example: the car park you use for work, the supermarket that delivers your weekly groceries or even the local pizzeria. Request to pay could give customers control over the internet of things by allowing them to control which requests to pay automatically and which request need approval from the account holder. By providing the opportunity of a one-click lifestyle request to pay and instant payments hold the promise of going mainstream and becoming part of our everyday lives.

03

REQUEST TO PAY: THE CORNERSTONE OF THE DIGITAL PAYMENT REVOLUTION

AN EXPERT VIEW FROM BANKING CIRCLE

Michael Boel, Head of Local Clearing at Payments Bank, Banking Circle

Request to pay, also known as R2P and RtP, is a new secure messaging service designed to make payments simpler and more flexible for businesses and consumers, as well as cheaper and easier to manage for the financial institutions and merchants involved in the payment journey. Alongside buy now pay later (BNPL), R2P is emerging as a cornerstone of payments in the digital era.

Complementing existing payments infrastructure, sitting alongside Direct Debit (DD) and other payment methods, R2P gives companies that have, historically, relied on invoicing for payment – and all the time, admin and delays that entails - the ability to turn the tables and request payment for a bill. The advantage for the seller is clear; the advantages for buyers are also considerable. On receiving a 'request to pay', a customer can quickly and easily pay in full or in part, opt to communicate with the biller, ask for more time or even decline to pay. And this means more flexibility and control over how they manage their finances.

Around the world, R2P is in its early days – according to a recent study fewer than one in five European banks currently offer R2P solutions although this is expected to reach one in two by the end of 2023. But as a payments innovation that is fit for purpose for the future it is already showing tremendous growth, indicating the enormous appetite for a flexible, low cost and secure new way to manage regular or one-off payments.

The global picture

In the UK, R2P is **PayUK**'s inaugural output, with the organisation quoting impressive economic benefits: "It is estimated that it could save the UK economy £1.3 billion per year. However subsequent research to that which was carried out in 2016 and 2017 would now suggest that this is a conservative figure, and it is more likely to be between £2 and £3 billion."

UK fintechs and banks have launched R2P offerings for invoicing, personal and Peer-to-Peer (P2P) payments, with R2P seen predominantly as an opportunity within the business-to-consumer (B2C) and consumer-to-business (C2B) fields, especially within e-commerce. However, in Northern Europe the peer-to-peer capabilities of R2P are being used where relatives are asked for money, or to pay bills. Denmark is a great example of this use case.

Currently most R2P schemes are built as a national model designed to be connected to regional interfaces such as P27 in Northern Europe. Indeed, R2P frameworks are already established in the UK, EU, Australia and the Nordics with one US scheme having gone live in 2021 and second estimated to go live in 2023.

In some regions, and when coupled with instant settlement, R2P is used as an alternative to DD. However, whilst this is a potential use in some specific cases, it is not wholly accepted and cannot compete directly with the classic use of DD – certainly not before R2P and open banking allow mandates and recurring payments. In situations where DD is used as an alternative to card payments, however, we do expect to see R2P rapidly gaining momentum in the coming months and years.

In the UK banks and consumers view DD as a superior payment solution due to the security and convenience it provides by making payments invisible: the due date is scheduled and automated. It will take time, therefore, for R2P to gain ground in the UK market that is currently held by DD. The picture is different in Portugal, though, where DDs are perceived as 'suffered' by the consumer. In Germany, SEPA DD is preferred even as a payment method for e-commerce.

Most regions are utilising a convenient one-to-many platform for merchants and banks [...] providing a central overview of transactions and real-time insights into flow of funds.

Most regions are utilising a convenient one-to-many platform for merchants and banks, through which banks access a suite of standardised, robust R2P services. The platform model empowers payer and payee by providing a central overview of transactions and real-time insights into flow of funds. Another option, however, is where payments are handled via a single integration between a third-party provider and the bank's API architecture.

Customers provide the third-party with their username and password for each transaction, and the third-party accesses the bank account to retrieve the funds. Exchange of funds occurs via the same rails as if the customer made the transfer themselves, and security is assured by the requirement for the customer to input their bank log-in details for every transaction.

Security and cost benefits

R2P offers many advantages for banks, merchants and their business and consumer customers, but security improvements are probably some of the most important benefits. Consumer authorisation happens within a bank's app or website, meaning that R2P transactions are protected by bank-level security. This can include two-factor authentication and the Strong Customer Authentication protocols mandated by the EU's second payment services directive (PSD2), where appropriate.

Also valuable for merchants, is the lower cost of R2P versus card payments. For businesses currently reliant on card payments, R2P offers an alternative that bypasses the card rails and associated interchange fees, dramatically reducing the cost per transaction.

Consumers and businesses alike are also attracted to R2P's potential for instant settlement, although that depends on the method adopted by the banks involved in the transaction. R2P is already proving popular for speeding up the cashflow of micro merchants and 'gig' economy workers, and for removing the friction in bill payment for the 18-34 demographic.

All part of the digital shift

R2P clearly demonstrates the potential of a flexible payment system based on Open APIs and designed to fit the needs of users in the digital era. It fits perfectly within the industry-wide shift to digital services, providing a more accessible payment solution. It makes sense, therefore, that banks looking to modernise their payment platforms by launching R2P solutions decide whether to adopt the third-party or platform approach.

National and international one-to-many platforms will prove cheaper and more efficient than integrating third parties... They will also be more easily connected across borders.

It is likely that the national and international one-to-many platforms will prove cheaper and more efficient than integrating third parties, as already being demonstrated in the Nordic and UK schemes. They will also be more easily connected across borders, bringing vital interoperability capable of increasing both the potential and the use cases of R2P.

It will undoubtedly take a few years to reach its potential, but once R2P is adopted and secured it will have the capacity to become an international payment model. And linked to digital and mobile uses, it is likely to represent a viable alternative to international payment schemes.

04

FORM3

RE-PLATFORMING CRITICAL PAYMENTS INFRASTRUCTURE TO THE CLOUD

AN EXPERT VIEW FROM FORM3

Michael Mueller, CEO, Form3

From mainframes to cloud

Like many century old industries, financial institutions established their organisational structures around a physical space, the office. The infrastructure needed to handle their critical business functions followed suit, and with the first computers being the size of a room, it seemed natural for the computer to live in a physical workspace.

Fast forward to the 1990s, server-rooms became the technological pulse of business, with every trade, payment, deal and email relying on it. With advances in technology moving at a rapid rate, so too did the demand for banks to digitalise their offerings. The multitude of business software needed was becoming as large as the hardware to manage it with offices being homes to endless racks of servers that continuously called for updates and maintenance.

In response to advances in technology and growth of digital, software hosting became the new normal with datacentres popping up all over the place enabling banks to host their business applications. Several decades later and this still continues today for many financial institutions around the world.

However, the advent of cloud has seen a steady adoption of cloud-based services, that have now become mainstream across multiple industries. Now we are seeing the adoption of cloud for the very services at the core of banks, including payments. On the latest leg of this journey, cloud native technology has become the new standard for managing and deploying applications which are built for the cloud from the ground up.

However, the advent of cloud has seen a steady adoption of cloud-based services, that have now become mainstream across multiple industries. Now we are seeing the adoption of cloud for the very services at the core of banks, including payments. On the latest leg of this journey, cloud native technology has become the new standard for managing and deploying applications which are built for the cloud from the ground up.

In today's new, everything instant world, offices have turned virtual and organisational structures are built around web not physical addresses. No longer do banks need to keep hosting and maintaining their ageing software applications in the cloud but can remove the infrastructure burden completely by outsourcing the entire payment processing, clearing and settlement to a cloud-native, payments-as-a-service platform instead.

Why re-platform?

With the continued rise in both adoption and volume of instant payments the direction of travel in this space is clear: towards an always on 24/7 payments landscape. This increased need to be able to process payments in real-time as well as scale capacity to accommodate the significant growth in payment volumes puts a tremendous strain on traditional back office technologies.

Unfortunately with this increase in volumes of payments comes with it the inevitable increase in potential fraud. Whilst it is often touted 'a payment is a payment' banks now need to ensure their own payments become 'smarter'. The ability to implement new technologies like real-time fraud screening or overlay services like 'confirmation of payee' is key to avoid the weaknesses found in traditional payment systems that can be exploited by fraudsters – a trend we are seeing more and more in these times.

Year on year, as customers expect ever more reliable, easy to use digital offerings from their banking services (with challenger banks setting out the realities of the art of the possible), legacy banks look to improve their services to rival that of the challengers.

All financial institutions running on legacy technology are currently facing the same problem: they need to re-think legacy architectures that are increasingly costly, risky to maintain and slow to develop. Year on year, as customers expect ever more reliable, easy to use digital offerings from their banking services (with challenger banks setting out the realities of the art of the possible), legacy banks look to improve their services to rival that of the challengers.

They then face the problem that their legacy infrastructure, already outdated after a lengthy implementation, is based upon decades old technology that is hard to update. Increasing or decreasing physical capacity isn't possible so increases in demand lead to downtime for customers. When updates are planned for the scheduled downtime inevitably impacts customers. Finally, banks that are tasked to operate and update these systems in the face of regulatory changes and scheme updates are inevitably over-reliant on the expertise of the original implementation teams whose professional services fees reflect this harsh reality.

By moving to a 'cloud-first' platform banks can now access the functionality and speed to market now required to adapt and survive. They need to be architected differently, from the core foundations up if they want to really benefit from new banking and payments services. This doesn't simply mean technologically; they need to be architected for constant change across the organisation, from the way they interact with their customers to the way they develop, test and deploy code.

Through embracing re-platforming to the cloud, banks will be able to:

- Accelerate their speed of transformation to a future proofed platform.
- Enable transparency over their Total Cost of Ownership (TCO), whilst improving their return on investment through accessing a more reliable service at lower cost.
- Improve availability, resilience, and scalability that takes full advantage of cloud native microservices and the potential for cloud-agnostic configurations.

Banking software of the past is predominantly based on mainframe services architecture. The software itself is a large program with one input point and one output point. If you need to add new capacity it is a case of linear scaling, you need to add more servers to run more instances of the software in order to have more capacity, or sometimes the only option is to scale vertically by upgrading the servers. Such tasks are traditionally manual and can take months to complete.

This means more material cost to deal with higher demand, potentially downtime and a physical process of increasing your capacity. Thus, the critical infrastructure and one of the core components of every banks output (the ability to send and receive money) is based on physical infrastructure that isn't able to adapt.

Removing barriers to change

With financial institutions being aware that their current payment processing capabilities are unlikely to be fit for purpose in the near future, they then have a whole new challenge to solve: not only transitioning the technology and creating a more sustainable operating model but transitioning the organisational mindset, its structure, its teams and in doing so, its business agility.

This is completely different to the traditional command and control governance, waterfall delivery, of so many large banks. Questions of risk and regulatory scrutiny are very important; with Banks being a critical part of nationwide infrastructure even a small risk of a service blackout is enough to bring transformation projects to a halt.

Culturally, there needs to be a shift from 'the old ways' to a new way of working which requires a mindset change across the organisation. Moving critical payments infrastructure to a PaaS model will vastly improve the technology capability but also optimises processes and crucially changes organisational thinking. And that means spending time on the clarity of purpose, gaining buy-in and thorough design as well as organising collaborative teams to build a sufficient plan around testing and control mechanisms that enables a smooth transition with fewer bumps in the road.

Back-end platforms as enablers of front-end innovation

Huge advances in technology innovation are transforming the very core of financial services, challenging banks to reassess their front- and back-end platform architecture. It is not surprising that financial institutions around the world have started to examine payment platforms and the capabilities of the cloud as a key first step in moving away from the restrictions and barriers inherent in their existing legacy payment solutions.

One of the key reasons that platform technology can be so effective is its agility. A central element of this is the speed with which the systems can be improved. Paired with the power of the cloud these new agile back-end systems can provide banks the ability to upgrade and enhance on a monthly basis as opposed to previous yearly timeframes. This platform agility is the foundation on which the payment innovations of tomorrow will be built.

05

FROM OPEN BANKING TO OPEN FINANCE

AN EXPERT VIEW FROM CBI

Liliana Fratini Passi, CEO, CBI

Over recent years the global payment landscape has changed radically, with consumers increasingly turning to digital solutions. Due to the reduced use of cash, increased knowledge and confidence in digital payments, customer demands have reshaped the banking and payment industry, beyond the regulatory obligations of the PSD2 directive, requiring banks to innovate both in terms of technology and mindset, in order to remain relevant and competitive, against expanding fintech and BigTech operators.

Embracing the technological revolution

Consequently, banks have needed to review their traditional business models and embrace the technological revolution, through new partnerships with market incumbents and newcomers in the field of innovative technologies, which provide for new VAS for consumers, in what has become a data driven, transactional and networked economy.

In this scenario, open banking has both fostered digitalisation and a cultural awakening towards the benefits of new collaborative ecosystems, in which the interconnectedness of each player can gain and contribute to sustainable, circular economic growth and value creation, through enhanced services, increased frictionless and secure functionality and interoperability. It is clear that in what remains a rapidly changing market landscape, in which disruptive innovation is both increasing competition and blurring industry lines, open banking not only represents a 'win-win' scenario for banks and customers alike, but an inevitable first step towards open finance.

Irrespective of whether open banking has been driven by regulation or market players, and its state of maturity and approach taken, open banking represents a global phenomenon, with over 60 countries adopting open banking and open data measures, and an estimated 24 million users worldwide.

Notwithstanding these statistics that highlight the potential of open banking, the Italian market is lagging in realising the full and transformative nature of open banking, and its contribution to meeting current and future customer unmet needs.

Notwithstanding these statistics that highlight the potential of open banking, the Italian market is lagging in realising the full and transformative nature of open banking, and its contribution to meeting current and future customer unmet needs.

To this end, and until recently, a short-sighted approach of open banking was adopted in Italy, focusing on regulatory compliance of the PSD2, rather than on the positive value, or the disruptive consequences of innovative technologies to the financial services industry.

The emergence and diffusion of new data sharing models

The international emergence and diffusion of new data sharing models, supported by innovations such as decentralised transaction validation technologies and biometric identification systems, all point to further disruption in Financial Services, with a distinct possibility and opportunity of open banking transitioning towards open finance. The EU digital finance strategy and UK's FCA Open Finance Consultations of 2021, all point in this direction.

While open banking in Italy is still in a nascent phase, banks and financial intermediaries that wish to retain market share, will need to rapidly strengthen collaborations with third party and technical providers, so that they are able to deliver a broader range of financial services to customers.

The agenda therefore moves from connecting application programming interfaces for the purposes of payments, to sharing different-if not all-layers of customers financial data over a shared network that which ultimately lead to greater transparency, competition, and customer choice.

Building upon the advancements in secure data sharing technology that have created digital payment ecosystems, our goal is that of layering shared functionality over a broader set of data, thus connecting products and services, which simultaneously create a new level of openness and permit a wider financial footprint.

It is thus clear that open finance is the next level of disruptive innovation in the financial industry, which banks will necessarily need to endorse to match the position of trust they currently enjoy with that of a competitive player in an increasingly transactional and digital marketplace.

06

GOCARDLESS

THE ROLE OF OPEN BANKING IN THE FIGHT AGAINST RISING PAYMENT FRAUD

AN EXPERT VIEW FROM GOCARDLESS

Siamac Rezaiezadeh, Director of Product Marketing, GoCardless

According to new research by the Merchant Risk Council (MRC), the global cost of payment fraud has increased for a second consecutive year. Mid-sized organisations (those ranging from $5-50million in revenue) have been hit the hardest, with significant spikes in domestic and international eCommerce orders that transpired to be fraudulent, as well as spikes in the percentage of eCommerce revenue lost to payment fraud globally. Whilst clearly on the rise, payment fraud is not a new phenomenon, rather it has festered under the surface long before payments were digitised.

GoCardless' own research echoes that of the MRC's findings, with 41% of businesses agreeing that payment fraud is an extremely large problem for their business and a further third saying that fraud is amongst the top threats that they face. This doesn't appear to be for lack of effort from businesses - in fact, quite the opposite. On average, merchants use two to three different techniques to optimise payment authorisation and employ three full-time team members just to manage fraudulent payments and payers. It's why the real cost of fraud isn't just the revenue lost - it's the admin, the resources, the time. It quickly adds up, with one in four companies feeling frustrated by the amount of time they still need to put into fraud management, even when they have tools in place.

Payments are broken

Despite best efforts, it's clear that the current fraud-fighting methods are not yielding the desired results. What's more, businesses have had to choose from payment solutions that either come at a higher cost, offer a low ROI, or add friction to a customer's checkout experience. Let's take cards as an example; paying by card has become a lot more painful since the implementation of the newly enforced Strong Customer Authentication rules, with the security measures adding friction which we predict will impact customer churn and new payer sign up rates.

Despite being an excellent payment method for recurring revenue cases, Direct Debit also has its drawbacks. Yes, it has low transaction fees, high payer preference and low payment failure rates, and GoCardless has seen first-hand how switching from card to bank pay has helped businesses to reduce churn and improve cash flow. However, this doesn't mean that Direct Debit isn't without its associated risk, with no additional authorisation steps currently in place to verify payer information.

There are varying degrees of vulnerability depending on the merchant use case, with high volume subscription businesses being at the higher end of the risk spectrum. This is because:

- They are onboarding hundreds, if not thousands, of new customers every day, making manual account validation impossible, and
- often merchants are stuck in a paradox of choice between pre-emptively protecting revenue or providing a positive customer experience by instantly sending out a customer's order.

Using open banking to re-imagine account verification

Open banking APIs provide a gateway to untapped data. Verified identity information, current and historical bank account balances and transactional behaviour can now be incorporated into risk models to provide much more accurate risk profiling. Open banking data is especially powerful when combined with bank-to-bank payments, taking the best of the existing Direct Debit benefits and making them even more secure than other payment options.

The next phase: making fraud prevention intelligent

Should businesses use open banking to verify bank details, even in the few cases where fraud is more of an inconvenience than a significant problem? Put simply - yes. It's rare that businesses don't have the ambition to scale and, without the proper payments strategy in place early, inconveniences grow to become issues. But as the proverb goes, businesses shouldn't put all of their eggs in one basket. Yes, bank account verification will ease the current pressures of fraud, and also demonstrate once again the ever-growing value that open banking can provide when utilised correctly.

But there isn't just one type of fraud that businesses need to manage and minimise. The next step is something that we're already working on, exploring how open banking can be combined with payment data to not only verify accounts but to also predict upfront whether a payer is likely to be fraudulent, monitor for suspicious activities after an account has been set up, and to also challenge unfair chargeback activities. This type of innovation doesn't happen overnight, but with fraud currently costing the global economy over $5 trillion each year, it will be worth the wait.

07
BUILDING OPERATIONAL RESILIENCE

The Covid-19 pandemic and Russia's invasion of Ukraine are two highly relevant recent examples which underscore the need for greater operational resilience (OR) across financial services.

Aimed at developing a far more resilient financial system that can absorb and manage shocks rather than exacerbating them, operational resilience has become a key focus for regulators over the past few years. Given the rapid digitisation of financial services, the highly interconnected nature of the system means that there is a far greater exposure to impact from operational disruptions, with significant risk of crippling knock-on effects.

Equally, with such technological evolution, regulators, central banks and the private sector are better positioned to leverage tech tools which reinforce their systems than ever before.

How banks should prepare for the OR reset

Simon Treacy, senior associate, Linklaters, explains that financial institutions (including payment service providers) across the EU and UK are being asked to take a new approach to withstanding disruption. "Both new and incoming rules on operational resilience require financial institutions to anatomise how they provide their business to their clients. The gauntlet for firms to take up is to identify where operational risks lie and prepare to manage those risks when (not if) disruption strikes."

> *"'"Both new and incoming rules on operational resilience require financial institutions to anatomise how they provide their business to their clients. The gauntlet for firms to take up is to identify where operational risks lie and prepare to manage those risks when (not if) disruption strikes."*
>
> **Simon Treacy,**
> Senior Associate, Linklaters

Treacy notes that the EU and UK are at different stages in the regulatory process, with the UK currently leading the way. The Bank of England, Prudential Regulation Authority and Financial Conduct Authority have set rules which started to take effect on 31 March 2022, although certain aspects do not apply in full until after a three-year transition period.

"If you take that transition period into account, the EU is not far behind. Its proposals for a Digital Operational Resilience Act (DORA) are currently wending their way through the EU's legislative process."

Negotiations on the final text should be completed later this year and the rules should start to take effect before the end of 2024.

Both the EU and UK regimes set a more prescriptive process for anticipating operational disruption. For example, Treacy elaborates, the UK regime spells out exactly what documentation in-scope firms are expected to maintain.

These documents should not only evidence compliance with the operational resilience rules as a whole, but also "show their working out" by justifying decisions made during implementation. This suite of documentation must be available to the regulators on request. As a note of warning, Treacy adds that in many cases the regulator will review these papers for the first time in the wake of an incident, and with the benefit of hindsight.

Adam Stage, senior manager and operational resilience practitioner for TSB Bank, furthers that the policy and supervisory statements on operational resilience and third party risk management (including outsourcing) are live in the UK, and most financial institutions are focusing on how they continue to mature their approach and embed resilience practices within their business-as-usual operating model.

"This means increasing the sophistication of how they map their services and test their resilience, and also how to maintain the resilience assessments and monitor that agreed actions are being done, all in an efficient way. Of course, financial institutions are also curious about what others have done and how they compare against their peers, and here discussions with supervisors and public speeches, like that by **David Bailey of the PRA**, can help."

Echoing Treacy's observations about the prescriptive nature of OR regulations, Stage elaborates that in the lead up to the new regulations going live, regulators have reminded the industry that the policies would be principles-based and outcomes-focused, meaning that firms cannot rely on regulators giving them the answer.

"Instead," Stage continues, "firms would have to interpret the rules and guidance in a way which makes sense for them, and would need to articulate this confidently to their Board, to get their approval on the approach, and ultimately with their supervisors. Ensuring you have the right people engaged internally, and the right challenge along the way through your second line, is a great way to build this confidence."

For firms with international footprints, Stage notes that they should be looking at new expectations being set in other jurisdictions, including the DORA which is likely to come next. "Forming a clear view of the main components of each piece of regulation and where firms can 'undertake an activity once and use it many times', is important from an efficiency and also a consistency perspective."

The UK's impending consumer duty final rules present another key deadline for firms operating the UK according to Roger Tym, partner, Hogan Lovells. Firms won't have long after the publication or the final rules to prepare or make necessary changes.

Tym argues that to meet OR requirements, in scope firms should have identified their important business services, set impact tolerances and assessed how they will remain with tolerances. "Going forward, they should be undertaking the necessary investment and resource allocation to resolve any areas of potential weakness they have identified. In scope firms will also need to have brought their outsourcing contracts and arrangements in line with EBA guidelines.The review of end to end customer jouneys that will be needed to meet new Consumer Duty requirements (which the FCA have said will need to be implemented by the end of April next year) and firms will need to reassess their overall operational resilience plans."

Broadly speaking, explains Treacy, OR impact tolerance levels represent the point at which disruption causes a risk to market integrity or intolerable harm to customers. In-scope firms are required to remain within their impact tolerances for important business services by no later than end-March 2025.

How is technology helping banks with their OR strategy?

Technology-based tools intended to provide a solution to manage all of a bank's operational resilience needs are increasingly available, observes Stage. For the most part, these appear to be data repositories which provide a convenient way of storing information about your important business services in one place.

"These tools will likely be most helpful where they can integrate into firms' existing management frameworks such as their risk registers, or their business impact assessments (for business continuity), or their IT configuration management database (CMDB). A key area of focus for firms at the moment is identifying the right tool to maintain the maps of the IBS in an efficient manner and in a way which enables firms to identify vulnerabilities in their delivery model."

Conversely, senior director at Hogan Lovells, Frank Brown, argues that with firms increasingly hosting systems on the cloud across multiple availability zones they could be forgiven for thinking this addresses their operational resilience requirements.

> *"It is important for firms to remember that a robust approach to operational resilience also requires consideration of key third party suppliers (and identification of potential alternatives), the robustness and security of connections, system back-ups and post-implementation testing and a roll back approach in case of issues."*
>
> **Frank Brown,**
> Senior Director, Hogan Lovells

"It is important for firms to remember that a robust approach to operational resilience also requires consideration of key third party suppliers (and identification of potential alternatives), the robustness and security of connections, system back-ups and post-implementation testing and a roll back approach in case of issues."

Brown continues that firms also need to ensure they have a deep understanding of how their customers use the products to identify which aspects of the service are important.

"Regardless of the tools used to support operational resilience firms need to be sure their process, approach, oversight and testing are sufficiently robust and understood by senior management," Brown states.

Can true operational resilience be inconsistent?

Stage believes that The Basel Commission on Banking Supervision (BCBS) will be key in driving a common approach to operational resilience around the world.

"I agree with the **PRA's view** that the UK and BCBS approaches align on the core principles, and the existing US approach is similar too."

These approaches are effectively driving firms to define those services where an operational disruption would be most impactful, through external as well as internal lenses, i.e. the impact on customers and markets as well as the firm's own financial viability. The approaches require firms to deepen their understanding of how the services are delivered (through mapping), to set a tolerance for disruption, and to test their ability to remain within those tolerances.

Matthew Handfield, principal consultant, Hogan Lovells, says similarities across jurisdictions include the need to consider the products and services on offer, including how they are used by customers, to understand what is important, a robust approach to oversight of third parties and having a plan in place for when things go wrong, including the approach to communication during a service interruption.

Where jurisdictions diverge is on the interpretation of exactly what parts of the business are considered important. "However, a robust approach to operational resilience is not only something to demonstrate to regulators; it is key to providing a reliable service and building customer trust," and going beyond the bare minimum of regulatory compliance is wise.

While several aspects of DORA echo the UK regime, notes Treacy, such as the proposed requirements around testing, documentation and governance, divergences remain.

> *"One significant difference between the two regimes is that DORA does not have a strict liability standard requiring firms to remain within impact tolerances – something which is at the heart of the UK rules."*
>
> **Simon Treacy,**
> Senior Associate, Linklaters

"One significant difference between the two regimes is that DORA does not have a strict liability standard requiring firms to remain within impact tolerances – something which is at the heart of the UK rules."

Another difference Treacy points to between the two regimes relates to scope. The UK rules apply to many but not all financial institutions, with in-scope firms including banks and payments firms. Conversely, DORA is likely to apply to all financial entities in the EU, although a principle of proportionality should mean that firms can take into account the size, nature, scale and complexity of their business when implementing the rules.

Treacy continues that DORA also proposes a new regime for some businesses which provide IT services to the financial sector. Tech firms, such as cloud providers, could be designated as being "critical" to the functioning of the financial sector and subject to oversight by EU authorities. There is no equivalent in the UK regime, although the UK authorities plan to open a discussion paper later in 2022 on applying operational resilience standards to critical third parties.

According to Stage, the main differences in those approaches seems to come down to the responsibilities of regulators in each jurisdiction (e.g. the FCA brings a strong consumer interest focus to the UK) and the desire to evolve an existing approach (BCBS and US) vs trigger a step-change in the approach (UK).

Handfield explains that the UK's approach to OR is arguably more holistic and forward looking, and is likely to deliver better outcomes for customers and counterparties than some other jurisdictions. This is because it is focussed not only on assessing the risk of failure, but in building more robust systems to recover more quickly from service interruptions.

Equally, it is arguable that the European approach is more fragmented, with different initiatives dealing with different aspects of operational resilience. Handfield cites the EBA guidelines on Outsourcing, EBA guidelines on ICT and security risk management, EIOPA guidelines on outsourcing to cloud, ESMA guidelines on outsourcing to cloud. "Viewed comprehensively, these will achieve some of the same outcomes – but do not give a comprehensive view. DORA is likely to provide a more consistent regulatory framework across sectors as this progresses through the legislative process."

Stage adds that DORA "is a different beast entirely" as it focuses on the management of ICT risk and third party risk as underlying capabilities, rather than looking through the lens of an end-user service. Getting these things right will make a financial institution more resilient to a point, but without applying the external lens of what is most important."

08
NEW MEANS OF CUSTOMER AUTHENTICATION

With the rising cost of living, and the squeeze on finances anticipated in the coming months and years, fraudsters are going to double down on their attempts to extract more money out of consumers. Unfortunately, it is the most vulnerable – who typically don't have a lot of disposable income – who are most at risk.

Matt Cox, head of digital payments, Nationwide, told Finextra it is the industry's biggest responsibility to do everything it can in the fight against this in the coming years.

A future with SCA

A positive step in the fight against fraud has been the implementation of strong customer authentication (SCA).

"Looking ahead, the benefits of SCA will be the extra protection it provides for consumers and for Nationwide's members," said Cox. "Now that extra authentication controls are in place, Nationwide's early data suggests we will see around 2000 fewer victims of fraud every month – and millions of pounds will be saved. That's 2000 fewer members at Nationwide who won't have to suffer the impact and the heartache of being a victim of fraud."

> *"Clearly, the monetary and the human benefits are huge, but these technological developments must be enjoyed by all. If merchants are not ready, or if there is a pocket of consumers who are not 'mobile active', the industry will need to provide alternative solutions."*
>
> **Matt Cox,**
> Head of Digital Payments, Nationwide

Clearly, the monetary and the human benefits are huge, but these technological developments must be enjoyed by all. If merchants are not ready, or if there is a pocket of consumers who are not 'mobile active', the industry will need to provide alternative solutions.

"If these successes are replicated across the industry, this will be a major step forward in the ongoing fight against fraudsters," argued Cox. "Yet, we need to focus to ensure that the residual number of consumers that are unable to pay for certain things online are not forgotten. We cannot walk away yet."

Drop-out-at-checkout: A knock-on effect

For all its security benefits, some argue that SCA will cause online retailers to lose out on some sales because of the additional friction that it imposes on customers.

"I appreciate this risk," said Cox. "But with secure journeys that are also slick, I don't think in the long run sales will tumble. Security is a huge priority for consumers – not just checkout speed. They want both. As we introduce these changes, yes, drop-out-at-checkout will be a thing, but it will be a declining problem. The fact that we are asking consumers to authenticate is good and it will become normal accepted behaviour."

However short-lived, the impact of drop-off-at-checkout may encourage some businesses to explore alternative online payment methods, such as mobile wallets, argue some commentators.

"While this is a driver," acknowledged Cox, "let's be clear – right now, App2app authentication is the best experience, the most secure, and the most used. It's also best for merchants. For the customers that can, I would recommend this is the approach they take. Nonetheless, we must recognise that not all issuers, banks or building societies have developed this option yet, so we do need to allow for other options."

"Increasingly, we're going to see use of mobile App2app authentication for higher risk transactions," Cox continued. "Bear in mind, this isn't all transactions online. It's a small proportion of the transactions that happen online because most sail through without the additional authentication checks. In my view, they will become ubiquitous in the next one or two years."

Simon Gilson-Fox, head of product and solutions, UK & I, Visa, said that consumers should be able to choose how they want to pay for goods and services: "If they want to use their card to make an online payment, and benefit from the security protecting their payment from fraud, we should make sure it's as easy as possible for them to do so which means delivering SCA in a way that doesn't force the consumer to abandon their purchase or find alternative routes."

Biometrics: The smoothest and safest path

Arguably, the simplest and most secure way to apply SCA is via biometrics. In the coming years, they will become ubiquitous in the payments space, predicted Cox.

"The world of biometrics, with its potential to combat fraudsters, is hugely buoyant. There are strong incentives for the industry-at-large to adopt these measures." Gilson-Fox added: "Research has shown that customers increasingly consider biometrics to be secure and easy to use. By integrating biometric elements into their SCA challenge design, issuers can drive both customer confidence and trust. Visa recommends one of two options for the 'main' SCA solution, both involve the use of biometrics. One, a mobile banking app plus biometrics, known as out-of-band, or two one-time-passcode, plus behavioural biometrics."

One of the most challenging cyberattacks for providers to overcome is authorised push-payment (APP) fraud, where a customer is tricked into authorising a payment to an account controlled by a criminal. Through behavioural biometric technology, firms can match, for instance, keystroke patterns to users' profiles to ascertain who is attempting to conduct a transaction.

This is proving so effective that "regulators have given their view that biometrics are robust enough to be considered one of the key factors providers should aim to be using within their overall toolkit," stated Cox.
The apex of customer authentication

As technology becomes increasingly invisible, the customer's experience will improve. While quite niche today, there are a few usage examples in the marketplace already of biometric cards. These combine chip technology with fingerprints to verify a cardholder's identity with unparalleled speed and accuracy. There are even forms of biometrics emerging that play a role in tracking pulse rates, thus blocking a fraudulent activity before it occurs. Iris recognition, combinations of voice and face, too, are being explored.

> *"There is a huge flowering of innovation in the payments space, No doubt we will see new and improved solutions coming to market, because the one thing we can be sure of is that fraudsters will always find new ways around the defences we deploy."*
>
> **Matt Cox,**
> Head of Digital Payments, Nationwide

“There is a huge flowering of innovation in the payments space,” claimed Cox. “No doubt we will see new and improved solutions coming to market, because the one thing we can be sure of is that fraudsters will always find new ways around the defences we deploy.”

Cox and Gilson-Fox agreed that criminals will constantly adapt to new security measures and will seek out the weakest link in the security systems of financial institutions. Any new digital system should be designed with security top of mind. Educational campaigns combined with technological measures will both be critical to raise security awareness among users.

The apex of customer authentication

As technology becomes increasingly invisible, the customer’s experience will improve. While quite niche today, there are a few usage examples in the marketplace already of biometric cards. These combine chip technology with fingerprints to verify a cardholder's identity with unparalleled speed and accuracy. There are even forms of biometrics emerging that play a role in tracking pulse rates, thus blocking a fraudulent activity before it occurs. Iris recognition, combinations of voice and face, too, are being explored.

“There is a huge flowering of innovation in the payments space,” claimed Cox. “No doubt we will see new and improved solutions coming to market, because the one thing we can be sure of is that fraudsters will always find new ways around the defences we deploy.”

Cox and Gilson-Fox agreed that criminals will constantly adapt to new security measures and will seek out the weakest link in the security systems of financial institutions. Any new digital system should be designed with security top of mind. Educational campaigns combined with technological measures will both be critical to raise security awareness among users.

09

CBDC AND STABLECOINS – MAKER OR BREAKER OF THE FINANCIAL SYSTEM?

Digital currencies are still in a nascent stage; the trajectory and impact cannot be known at this time. Despite this, many commentators are positive that linked digital assets like CBDCs and stablecoins will find a comfortable home in the banking system of the future.

Yet with recent events, like the crashing of UST and subsequent instability around other digital assets might have a number of onlookers feeling increasingly cautious over the future of linked digital currencies and relying on them in the future.

Infrastructure

There are a number of challenges that must be faced before digitally linked assets are implemented. Primarily, the problem of infrastructure. Many European countries are currently conducting some form of investigation of their CBDC, with the most advanced likely being Sweden's E-krona pilot. However, it is still unclear what infrastructure choices might be made for these coins.

Inga Mullins, founder and CEO of Fluency, commented: "At this time, central banks and commercial banks are experimenting with a whole host of technologies, approaches and system architectures ranging from variations of current digital banking systems to comprehensive decentralised systems." Mullins continued: "It is reasonable to assume that digital currencies will be designed from the outset to be fully integrated with currently existing fiat currencies regimes. Moreover, this integration will need to be made fully transparent at the beginning of the CBDC rollout process."

Soren Mortensen, director global financial markets, IBM argues that the infrastructure is in fact, there. His view is that "recent experiments with Banque de France have clearly shown that the new digital world can co-existing with existing market infrastructures like Target2-Securities. The technology is already there to fully integrate these two worlds. Industry adoption is not a technology issue anymore but more of a transformation of the target operating model for financial institutions that still needs additional analysis to ascertain the cost benefits, as well as managements' willingness to change."

Ville Sointu, head of emerging technologies at Nordea, believes that while central banks are showing positive actions towards CBDCs, what moves they will make is not clear: "It's the publicly stated goal of central banks to make sure potential future digital currencies they issue are seamlessly compatible with the existing commercial money system. How this will exactly happen is still an unresolved design question in e.g., Europe. For virtual currencies this path is a little murkier; it's unclear how a pseudonymous system can retroactively made compatible with the regulated monetary system."

> *"The rise in CDBC demonstrates the strides made in adoption by central banks, but this process has taken years and the consequences are yet to be fully determined. Like any or many new payments efforts, regulators and participants are cautiously engaging and evolving their practices as needed since the associated risks or impacts are yet to be fully defined."*
>
> **Mary Ann Francis,**
> Associate Partner, Payments, IBM

Mary Ann Francis, associate partner, payments at IBM shares this sentiment, she states that "the rise in CDBC demonstrates the strides made in adoption by central banks, but this process has taken years and the consequences are yet to be fully determined. Like any or many new payments efforts, regulators and participants are cautiously engaging and evolving their practices as needed since the associated risks or impacts are yet to be fully defined."

Regulation

Another challenge that linked digital assets face is regulation. Arvin Abraham, partner at McDermott Will and Emery, comments on this. "Several major jurisdictions, including the EU with its pending Markets in Crypto-Assets Regulation (MiCA), have proposed significant new legislation to regulate digital currencies, but these are not in final form and care should be taken to avoid gun-jumping to accommodate regulation that is yet to stabilise."

Sointu says that "MiCA tries to reconcile some of these issues through limitations on unregistered wallets and adding KYC requirements on virtual asset service providers, but risks remain difficult to mitigate."

Abraham warns of taking premature actions: "Time and resources can be wasted in trying to accommodate regulation that does not come to pass. On the flip side, having an awareness of potential developments can help steer business models on a path that avoids painful remediation efforts."

Sointu adds: “It’s important to keep an eye on how the central bank digital currency ecosystem and related legislation is developing even at these early stages. Actively taking part in pilots and tests as these projects progress ensures the best outcomes for parties involved as several iterations with diverse and active participation naturally results in a better result. The same applies to the upcoming MiCA regulation for virtual currencies and service providers.”

Benefits

Despite these challenges, commentators seem to be positive that CBDCs and stablecoins will find a comfortable place in the existing banking system. For Mortensen, “within a foreseeable future, we see CBDCs being fully integrated into the existing financial system.”

Mullins also summaries the potential benefits as “access to instant and cost effective cross-border money transfers; availability of sophisticated and bespoke financial products and services; and potentially programmable money.”

Abraham notes that digital assets like these, “have the potential to streamline payments and create significant efficiencies in speed of transacting, record storing, etc. All of this comes with the caveat that proper regulation and oversight is required, particularly in areas such as AML/KYC controls.”

Sointu also reports that: “From a technical standpoint CBDCs in particular might have some benefit in B2B commerce as it makes it possible to create a highly interoperable instant settlement mechanism even for smaller amounts. It’s not clear however that this feature would be available in all CBDCs automatically.”

Mortensen concludes that with CBDCs, “the central banks will be able to control their money supply by managing the existing one alongside the CBDC money supply, and the conversion of one to the other.”

Mortensen adds: “Digital currencies open-up opportunities for existing providers who can take on new roles, such as intermediaries for CBDC distribution to end-users or even issuers of stablecoins for specific purposes. It will be important to understand the various usages and benefits of digital currencies, to get engaged in various emerging initiatives leveraging these.”

Predictions for the future of CBDC

Given the burgeoning position of currency-linked digital assets, it is hard to know the exact positions they may take in the future, however industry players have provided some of their predictions for the future of these digital currencies.

Specifically looking at CBDC, Mullins anticipates that "the integration with CBDC will be achieved in several ways depending on the medium or the specific digital wallets which the end-user would like to use for payments. For example, for web-based payments used for online shopping, the integration can be achieved via a plugged native mobile or SDKs embedded in the banking app. We also expect to see the introduction of smart electronic cards like today's credit cards but with a dedicated microchip triggering CBDC transactions."

Mullins adds that "as end users become increasingly familiar with the benefits of CBDCs and integrate their use in their day-to-day activities, new products and services catering to both retail and commercial users will emerge to leverage the architecture of CBDCs. And in this environment, commercial banks will be forced to innovate and enhance their level of service if they are to retain these customers. In addition, there will be a shift in AML and regulatory procedures/laws to adapt to the new CBDC landscape and ensure illicit transactions do not occur.

"End users become increasingly familiar with the benefits of CBDCs and integrate their use in their day-to-day activities, new products and services catering to both retail and commercial users will emerge to leverage the architecture of CBDCs."

Inga Mullins,
Founder and CEO, Fluency

Mortensen emphasises that "in general, we are moving to a more digital world, with a decline in cash usage in established economies. Digital currencies will grow in importance in a more digitally enabled world, and central banks will have to change the way they manage their money supply fiat vs CBDC, as well as how they monies can be converted into more commercial currencies and back again."

Sointu concludes with an essential warning about the philosophical future of these digital assets. "It's critical that a level playing field is created in the digital currency space. Same service, same risk, same rules."

10 CONCLUSION

The future trends and strategic development of the European payments landscape will be discussed by the industry's most influential payments practitioners at EBAday in Vienna, Austria on 31st May to 1st June.

Digital transformation, open finance, CBDCs and stablecoins, real-time payments, request to pay, liquidity management, correspondent banking, fraud prevention and cybersecurity, payments as a service, KYC and digital identity will be covered over the two days.

Back in-person after two years as a virtual conference, payment technology specialists, heads of innovation and an array of banking executives are set to descend on the event. Attendees will be welcomed into the charming city to connect, network, listen-in to a schedule stacked with expert panellists.

Headline speakers have been revealed, with industry heavyweights lining up to lead panel discussions throughout the two-day event, and Rohit Talwar is raring to generate some buzz with his highly anticipated challenge speech. From the European Commission's PSD2 Review, to DORA, building diversity in payments, the Digital Euro and all things instant payments, attendees will be spoiled for choice with sessions to choose from.

11 ABOUT FINEXTRA RESEARCH

This report is published by Finextra Research. Finextra Research is the world's leading specialist financial technology (fintech) news and information source. Finextra offers over 100,000 fintech news, features and TV content items to visitors of www.finextra.com.

Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra's unique global community consists of over 30,000 fintech professionals working inside banks and financial institutions, specialist fintech application and service providers, consulting organisations and mainstream technology providers. The Finextra community actively participate in posting their opinions and comments on the evolution of fintech. In addition, they contribute information and data to Finextra surveys and reports.

For more information:

Visit **www.finextra.com**,
follow **@finextra**, email **contact@finextra.com** or call +44 (0)20 3100 3670

12
ABOUT THE PARTNERS

Banking Circle

Banking Circle S.A. is the Payments Bank for the new economy. As a fully licenced bank, free of legacy systems, Banking Circle enables payments companies and banks of any scale to seize opportunities in the new economy - quickly, at low cost.

Banking Circle S.A. is a modern correspondent bank committed to building a local clearing network for all major currencies, to deliver fast, low cost payments with no hidden fees for the beneficiary. It provides a suite of unique and award-winning banking solutions, including multi-currency banking accounts and Virtual IBANs, bank connections for local clearing and cross-border payments, all underpinned by market leading compliance and security.

Through bespoke, flexible, scalable and futureproof solutions Banking Circle S.A. is enabling financial institutions to help their customers transact across borders in a way that was previously not possible.

Headquartered in Luxembourg, Banking Circle S.A. has offices in London, Munich and Copenhagen.

CBI

CBI is a public limited consortium company, which comprises around 400 Payment Service Providers as shareholders. CBI, established in 2001 by the Italian Banking Association (ABI), over the past 20 years has been operating from a Business-to-Business-to-Customer (B2B2C) perspective; CBI has been working to facilitate the interconnection between different ecosystems, in particular offering Banks the step forward to a "network economy", where services and value stem from an increased number of interconnected users.

Over 80% of the Italian banking industry has chosen the CBI Globe platform, which streamlines the telematic dialogue among Payment Service Providers, Fintech, enterprises, and the Public Administration to achieve compliance with the renewed EU regulatory framework and play an active role in the Open Banking scenario. Thanks to the capacity to reach out to online bank accounts at the domestic and European level, CBI Globe makes it possible to create innovative solutions for its clients. From an Open Finance and Data Monetization perspective, CBI has developed a few value-added services (VAS) to strengthen the competitiveness of its clients. Among these products, it is possible to mention the Check IBAN service, which allows the online verification of the association between an IBAN code and a fiscal code or vat number provided by a natural or legal entity.

www.cbi-org.eu

Form 3

Form 3 provide Banks and regulated Fintechs across the globe an end-to-end managed payments service that delivers complete payment processing, clearing and settlement to the universe of payment schemes through a single API.

Our platform handles everything so you can focus more on serving your customers' needs and less on managing payments infrastructure.

GoCardless

GoCardless is the global leader in direct bank payment solutions, making it easy to collect recurring and one-off payments directly from customers' bank accounts through direct debit and open banking.

The GoCardless global bank pay network and technology platform take the pain out of getting paid for 70,000 businesses worldwide, from multinational corporations to small businesses.

Each year GoCardless processes more than US$30 billion of payments across more than 30 countries. GoCardless is headquartered in the UK, with additional offices in Australia, France, Germany and the United States.

For more information, please visit **www.gocardless.com** and follow us on Twitter **@GoCardless**.

Infosys Finacle

Finacle is an industry leader in digital banking solutions.

We are a unit of EdgeVerve Systems, a product subsidiary of Infosys. We partner with emerging and established financial institutions to help inspire better banking. Our cloud-native solution suite and SaaS services help banks engage, innovate, operate, and transform better to scale digital transformation with confidence. Finacle solutions address the core banking, lending, digital engagement, payments, cash management, wealth management, treasury, analytics, AI, and blockchain requirements of financial institutions.

Banks in over 100 countries rely on **Finacle** to help more than a billion people save, pay, borrow, and invest better.

Finextra

Finextra Research
77 Shaftesbury Avenue
London,
W1D 5DU
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com