



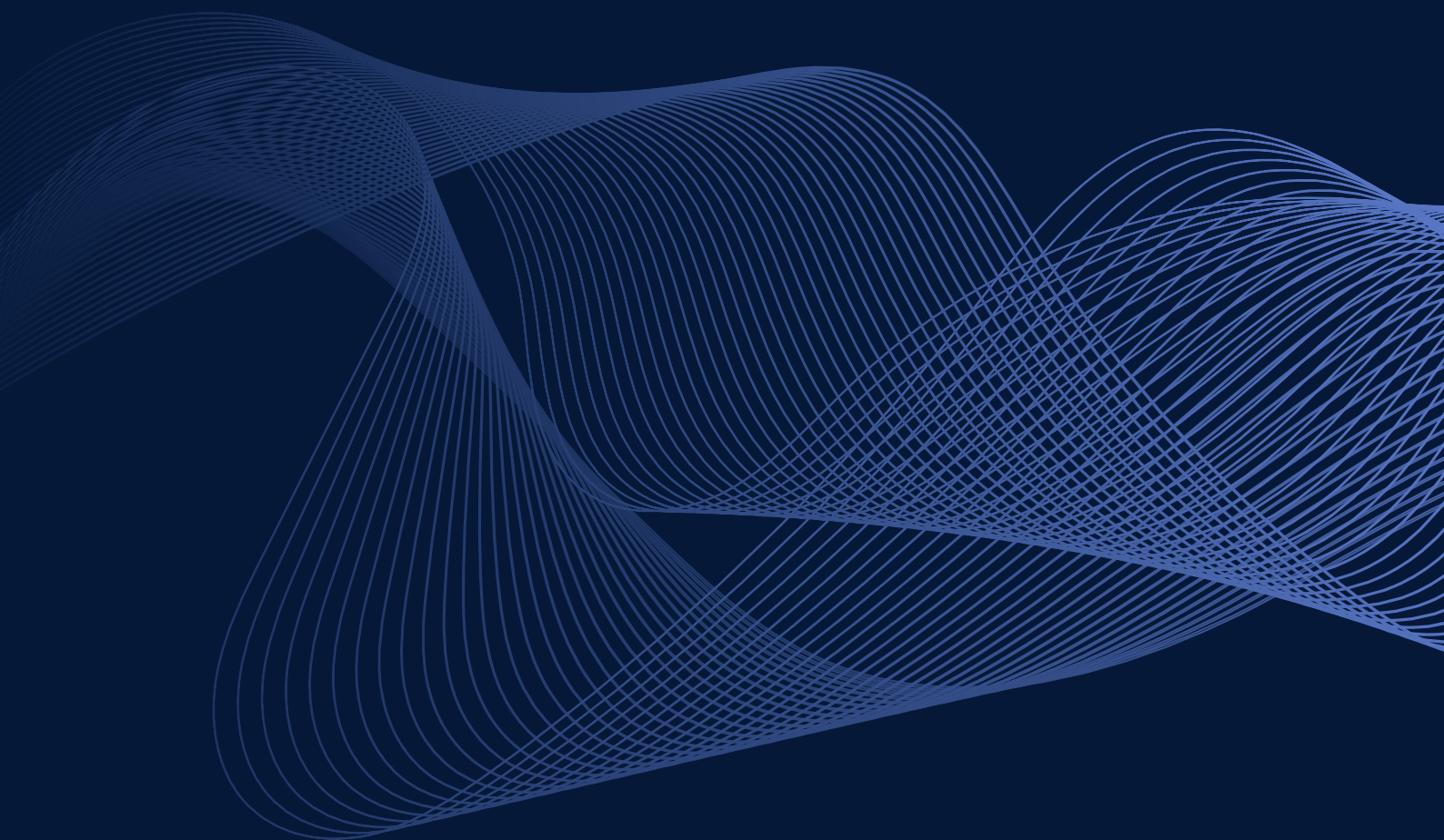
The role of the CDP in highly regulated industries:

Banking



Content

Foreword	3
The crux of the matter: Anonymisation and pseudonymisation	4
The role of the CDP in banking	6
Governance and consequences	10
Closing remarks	12



Foreword

There's no one who knows us quite as well as our banks. In fact, you could argue they know us better than we know ourselves—or at least better than we'd like to admit.

They see how we spend our wages—where, when, with which brands, and on what. They know our favourite coffee spots, our weekend indulgences, and even our travel habits. They see life's big moments reflected in our transactions—from weddings to growing families.

Money touches nearly every part of our lives, which makes our relationship with the institutions that manage it critically important.

The way we engage with our banks has changed dramatically over the years. Not long ago, visiting a physical branch, queuing with an account book, and hoping to withdraw cash before closing time was part of everyday life. If the doors were closed, so were our options.

Back then, we could speak to a bank manager who knew us personally and could make decisions on the spot. Today, those decisions often rest in the hands of algorithms.

The shift to digital has brought convenience—but it's also brought complexity. Banks are under pressure to meet rising consumer expectations while navigating a rapidly expanding set of digital platforms. At the same time, they must manage increasing regulatory demands and security risks. Every new interface and app can create new vulnerabilities.

But innovation shouldn't be slowed by risk. The challenge is to become smarter in how we use customer data—not just to protect, but to build trust, foster loyalty, and deliver better, more human banking experiences.

It's not easy. But it is absolutely possible.

The crux of the matter: Anonymisation and pseudonymisation

Before any discussion about the role a CDP can play within a highly regulated industry, it's critical to address the two core aspects of data management which define its effectiveness: anonymisation and pseudonymisation.

An understanding of these is especially key when balancing GDPR compliance with the ability to harness insight through data.

Anonymisation

This refers to the removal of all possibility to identify a specific customer through rendering it anonymous. The data involved is wholly detached from its subject and, as a result, can only be seen in absolutes. For example, anonymised data will show how many banking customers have expanded their portfolio of accounts from daily cashflow through to savings and ISAs.

In this regard, it can reveal macro trends within the entire customer dataset. But it won't allow a bank to know who has added an ISA on top of their current account, and therefore what other products or services might be of interest. Anonymisation can inform business strategy and where marketing might be working, but only from a top-down perspective.



Pseudonymisation

Solely using anonymised data will completely remove risk from handling customer data – but, as we've seen, it creates opacity and doesn't truly inform specific actions against insights.

However, introducing a pseudonymised stage to data management ensures businesses can personalise their marketing output, while staying GDPR compliant and safeguarding customer information.

In this process, individual customer data points are tagged with identifiers before analysis – “John Smith” becomes “BankCustomer001”, for example. Within the confines of the CDP, however, pseudonyms can be securely decrypted to uncover the specific individual and their contact details for the bank to reach out.

Marketing to identifiers

This means that the bank can understand the behaviour that BankCustomer001 demonstrates – their likes, dislikes, cashflow cadence, preferred stores, coffee shops, and where they go on holiday.

But, crucially, the bank only knows what that identifier does. It does not directly know that this is actually John Smith – the pseudonymisation of the data means the bank is GDPR compliant but can harness the power of the data it holds.

The upshot of such an approach means BankCustomer001 can be added to a marketing batch to receive specific promotions and offers – all of which are relevant, but none of which compromise privacy. Such an approach enables banks to share a known understanding with third parties and brands without any data breaches.



The role of the CDP in banking

CDPs and the win-win scenario

When we look at how a CDP can drive growth and customer loyalty within retail banking, we need to consider it within two mutually dependent remits.

Firstly, of course, like any consumer-facing industry, it needs to deliver against a commercial need. It has to increase the amount of money the customer is putting through their accounts, investing, and cross-selling to insurance and other products. This can be extended to brand and retail partners, where the data held by the bank can be used to inform promotions.

Secondly, this must act in tandem with supporting the customer throughout their life journey. The consumer is not the same person throughout their time with their bank, and loyalty can be driven through understanding their journeys and responding accordingly.

These combine to deliver greater customer lifetime value; through becoming an essential partner throughout life, the more money the customer will bring to the bank.

Data for loyalty

Consumers expect (indeed, demand) brands to offer promotions and special offers – they want to feel understood, valued, and important. It's the quid pro quo inherent in data sharing.

But it's fair to say retail banks – especially long-established high street banks – don't always deliver such VIP treatment. Given the data they hold about purchase behaviour and where money is spent, for banks to miss this opportunity could be considered commercial naivety.

Given that a customer's financial data must be handled with the utmost sensitivity, it could be easy to suggest that banks are being held back by an aversion to seeing it used for promotions.

Yet, on the contrary, our own research from 2021 identified a high appetite for promotions and special offers from banking partners, based on customer data.



Missed opportunities

Despite having a highly receptive audience, it's evident retail banks are not grasping the opportunity to hand when it comes to offering promotions and special offers. The survey found that three in ten UK consumer banks currently provide offers and promotions, yet two thirds of customers would trust their bank to provide personalised promotions.

Indeed, UK consumers are most likely to trust their bank (67% of respondents) to provide personalised promotions compared to their local supermarket (57%), the online retailer they use most frequently (54%) or their mobile phone service provider (52%).

To not act on this confidence is to miss a huge commercial opportunity. Brands need to understand the opportunity this openness brings when it comes to banks as a consumer channel – but it's up to the financial sector to lead this education process.

Secure analysis

This is a clear demonstration of where a CDP can offer banks the edge in becoming essential to customers and addressing potential churn.

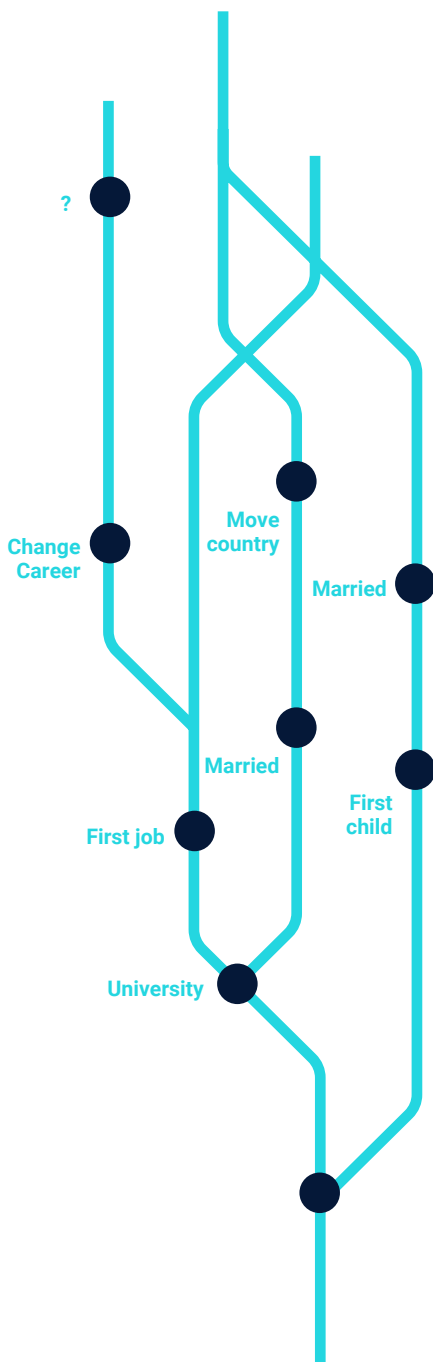
The high-grade security a CDP brings allows banks to analyse purchasing data and approach brands accordingly, knowing which specific (pseudonymised) customers regularly buy from them. In being able to take a partnership direct to known buyers, the banks in turn become an essential aspect of a marketing ecosystem. It becomes one of the most effective, highly targeted, direct-to-consumer promotions.

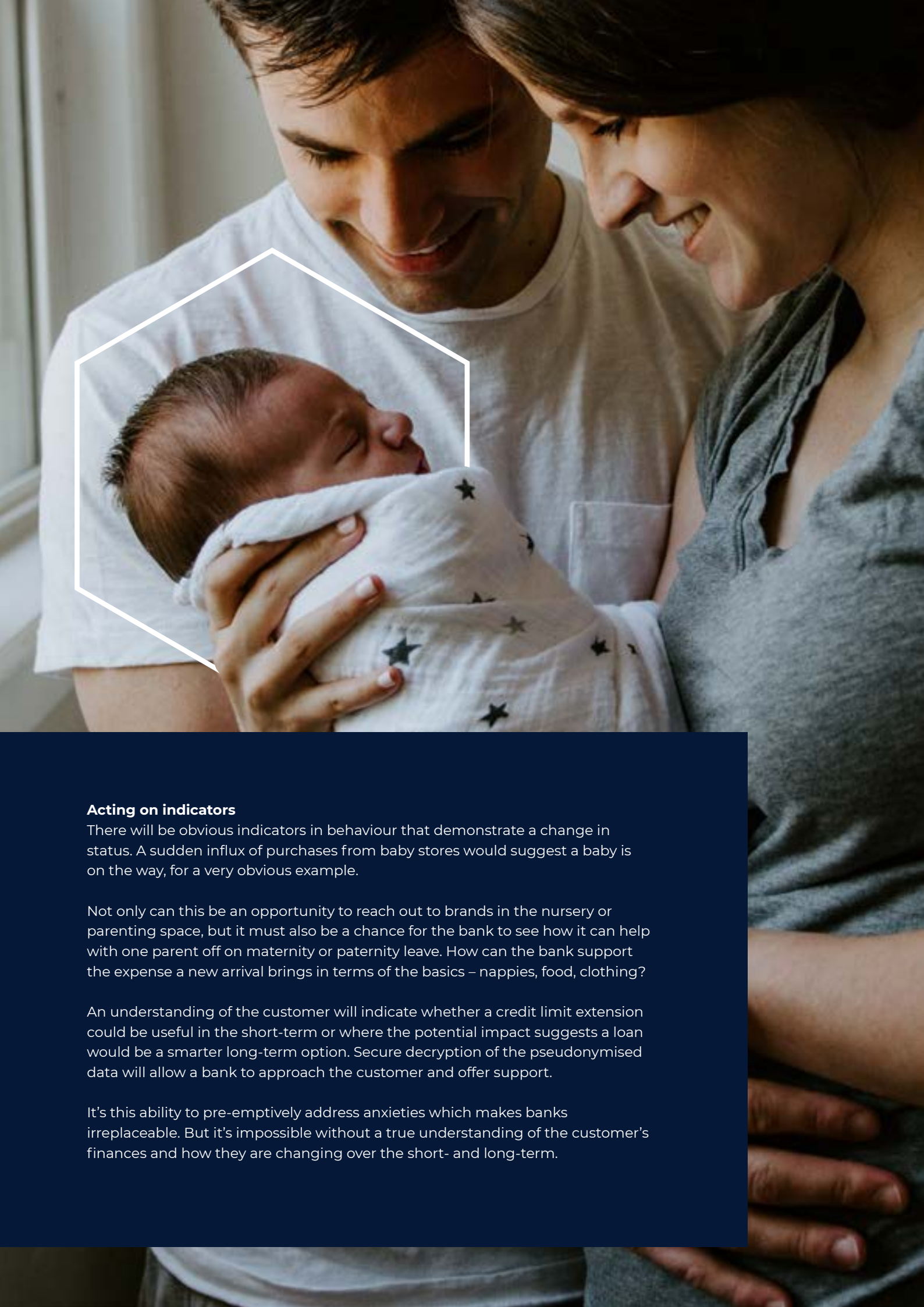
Regulatory aspects might also be a concern, however. Using data analysis to inform promotions, and the inherent sharing of opportunities with brands and partners, brings fresh compliance demands. But the ability to manage risk through a CDP means this compliance becomes a hygiene factor within the analytics.

The customer's 'life journey'

Every banking customer is intrinsically more than just an account number. They're a collective of individuals all on their own life path. No two lives are the same, and as such a bank must consider each of them as having a life journey, not just a customer journey. A traditional brand 'nurture programme', therefore, can't stand alone.

Banks need to understand where the customer is on their journey and, accordingly, what they need from the bank. Every path is different, but they share many of the same milestones: leave school, find a partner, buy or rent a property, children, retirement (albeit not always in this order).





Acting on indicators

There will be obvious indicators in behaviour that demonstrate a change in status. A sudden influx of purchases from baby stores would suggest a baby is on the way, for a very obvious example.

Not only can this be an opportunity to reach out to brands in the nursery or parenting space, but it must also be a chance for the bank to see how it can help with one parent off on maternity or paternity leave. How can the bank support the expense a new arrival brings in terms of the basics – nappies, food, clothing?

An understanding of the customer will indicate whether a credit limit extension could be useful in the short-term or where the potential impact suggests a loan would be a smarter long-term option. Secure decryption of the pseudonymised data will allow a bank to approach the customer and offer support.

It's this ability to pre-emptively address anxieties which makes banks irreplaceable. But it's impossible without a true understanding of the customer's finances and how they are changing over the short- and long-term.



The evolution of digitalisation

The opportunity to become a partner through the customer's 'life journey' is fundamentally based on the increased volume of data banks are gathering. This is a direct result of the rapid digitalisation the sector has witnessed in recent years and the expectation the customer has to engage with their bank across a variety of platforms.

In part, this has been driven by the explosion of challenger banks (many of which are digital-first) to the bricks and mortar high street models. The latter have had to rapidly evolve to keep pace with the digitally native former, who have the benefit of building highly intuitive services from the ground up.

This all means that customers expect an intuitive online experience across desktop, app, mobile, and tablet interfaces. With finances being such an emotive part of life, any fragmentation or lack of synchronisation will cause alarm. Ironically, instead of digital platforms becoming a positive differentiator, they became a source of dissatisfaction and potential churn.

The degree to which banks had progressed on their own digital transformation journey was highlighted during the pandemic. Estimates suggest that a previous 80:20 online to mobile ratio performed a wholesale flip to 20:80 within a matter of a few months. Mobile has become near default.

Aside from the behavioural change, it brought fresh regulatory challenges for banks. They were duty bound to reach out to customers to gauge how changing circumstances were affecting their finances, and support as necessary.

But the banks without fully functional digital systems discovered the degree to which (non-financial) customer data was held by third parties. All the data held by the banks was anonymised, so banks relied on information from external sources that held their customers' data when reaching out direct.

...In this instance, the 'duty of interest' meant that banks were able to take this data and use it as their own, pseudo-first party assets. Such a wake-up call could be seen as silver lining, but it shouldn't take seismic change to highlight operational failings.



Governance and consequences

The banking sector is one of the most highly regulated in the world – for obvious reasons. Regulators ensure not just that data and customer information is held securely (with significant fines and license revocations for breaches), but also that customers are protected against the impact of a banking transgression.

In the UK, the key players are as follows:

The Financial Conduct Authority (FCA) is the foremost body for the banking and finance sector. It acts on breaches and institutional failings due to a fundamental purpose of protecting the consumer and their finances.

The FCA has the power to ban financial products, publish details of misleading financial promotions, disclose duty of care failings, and will publish information about any disciplinary action being taken. Such action includes fines and even licenses being revoked.

Other bodies include the Payment Services Regulator (PSR) which is responsible for the oversight of all retail payment systems, and the Financial Ombudsman Service (FOS) which has the statutory responsibility to handle complaints and compensation claims.

The FOS has the power to settle disputes and lay down settlements. While an independent entity, it has a memorandum of understanding with the FCA and holds significant sway among retail banks.

Ultimately, HM Treasury has overall responsibility for institutional structure of banking and regulation, reporting to Parliament on serious problems in the financial system and the measures required to resolve them. It's important to note that the Treasury monitors the resilience of the banking sector and takes responsibility for handling operational disruption – something highly evident during the pandemic.



Mistakes made

Increasingly strict regulations are significantly reducing incidents in the sector when it comes to the misuse of data to protect the customer or inform banking operations. The majority of fines relate to anti-money laundering failings.

However, a Which? report in January 2022 identified poor governance on apps and online services. Negligence to implement sufficiently secure passwords and encryption featured prominently, as did insecure websites, which suggest poor infrastructure set-up. Arguably this could be a direct result of accelerated or rushed digital transformation processes by laggard operators.

Worryingly, inadequate login protection, app navigation, and ease of account management across platforms was an issue among the fifteen major banks researched. During the test, it was also identified that one challenger bank didn't ask users to login every time a user accessed their account. This can only be seen as a failure in a bank's duty of care.

There were banks which scored highly, of course, but the scale of these issues caused concern. The analysis has not yet resulted in any fines – it's not clear how the FCA is going to use the findings and act in due course.

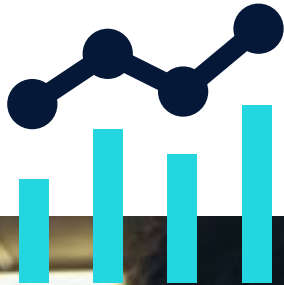


Closing remarks

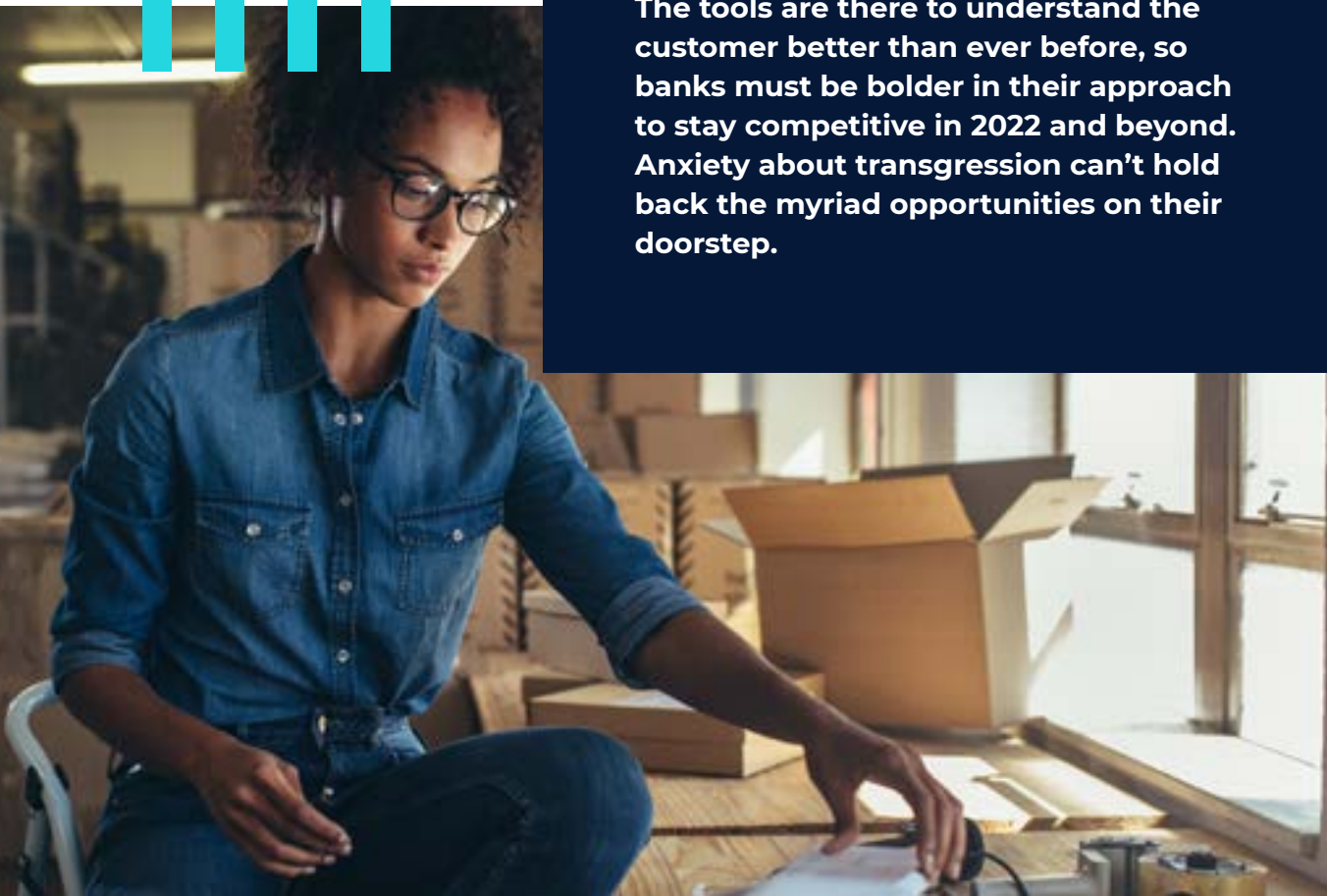
It's important to note that good news rarely makes the news. Poor infrastructure creating fractures and points of failure shouldn't be allowed to dictate a bank's behaviour. After all, rightful concern about the effect of operational difficulties must be resolved through addressing the causes behind them – which sit with technical and governance teams.

Rather, discussions internally must focus on how banks can become more agile with customer data, while complying with the strict regulations in place. Military grade security means complex data analysis can be allowed to flourish, which can allow banks to understand each customer better than ever.

Once established, such an understanding will make the bank a life-long partner – bringing with it growth in investments. It also allows the bank to position itself as an essential platform within any brand's marketing strategy – after all, consumers have shown the appetite for their data to be used for their own benefit.



The tools are there to understand the customer better than ever before, so banks must be bolder in their approach to stay competitive in 2022 and beyond. Anxiety about transgression can't hold back the myriad opportunities on their doorstep.





Tealium is a Customer Data Stream.
We are an intelligent real-time data streaming platform.

Tealium helps companies collect, govern, and enrich their customer data in real-time to power AI initiatives and delight customers in the moments that matter. Tealium's turnkey integration ecosystem supports more than 1,300 built-in connections from the world's most prominent technology experts. Tealium's solutions include a real-time customer data platform (CDP) with intelligent AI data streaming, tag management, and an API hub. Tealium's data collection, management, and activation capabilities enable enterprises to accelerate operating performance, enhance customer experiences, drive better outcomes, and support global data compliance. More than 850 leading businesses globally trust Tealium to power their customer data strategies.

For more information, visit

visit tealium.com