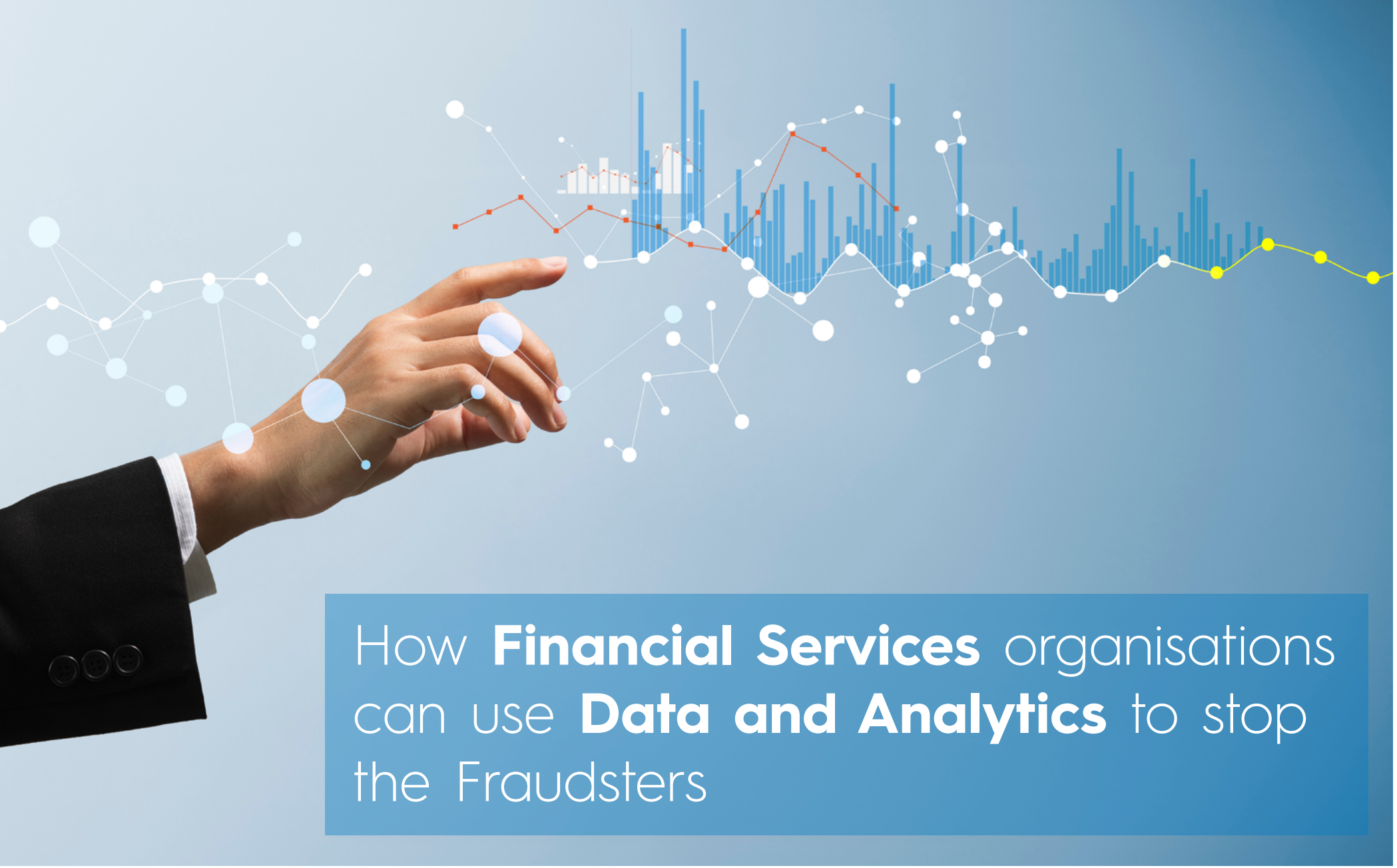


How **Financial Services** organisations can use **Data and Analytics** to stop the Fraudsters

The world is how we shape it

sopra steria

Introduction

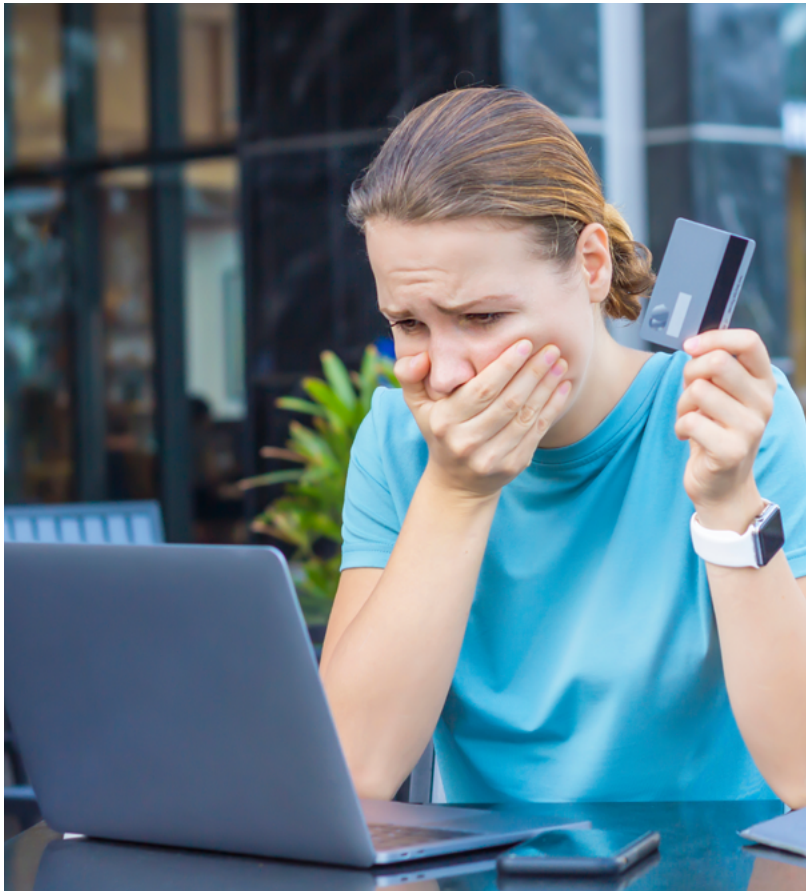
The battle against fraud is a worldwide problem and on a pan-industry-scale with macro-economic impact to Financial Services being of no exception and yet of key consideration.

In 2020, card-related fraud losses were rapidly reduced by c.£46 million – affecting mainly the younger demographics, with c.44% of those impacted being between ages 20 to 29 (more than double of those between ages 70 to 79 at c.20%).

The overall view on reported losses is much higher however, as an estimated £200+ billion every year is lost to fraud in the United Kingdom. Private companies are suffering most at an estimated £150+ billion, with the public sector adding a further £50+ billion. Personal fraud victims add another c.£9 billion with a further c.£7 billion due to unknown factors/ circumstances.

It is safe to say the situation is 'challenging' and the risk rapidly compounding year on year as more people and businesses connect, with platform development to facilitate the global electronic payment ecosystem becoming an industry within its own right.

The news is telling us the fraudsters are winning.
But at Sopra Steria we are thinking differently and have been working with several of our banking clients to help them fight back!



Understanding the fraud landscape

The fraud threat facing banks and payment providers continues to grow year on year. 'Which' estimates UK banks lose £700k per day or £29k an hour just through transfer fraud alone! Other indirect types of fraud obviously add to this figure. Vulnerabilities in payment services has due to digital and mobile customer platforms increased. New solutions leading to payment transactions being executed quicker, leaving banks with less time to identify, counteract, and recover underlying funds.

Sophistication of fraud is also increasing; fraudsters don't stand still. As soon as one loop hole is closed another opens along with a wealth of stolen data which is subsequently readily available for further criminal activity. According to *Privacyaffairs.com* credit card details with account balances up to $5000 can be bought for $240, while hacked Coinbase verified accounts reach $610 on the Dark Web, thus providing a rich marketplace for fraudsters and making the task of protecting their own banking customers even harder.

The accelerated digital shift of customers to new, digital ways of banking and transacting has allowed more sophisticated approaches by unscrupulous fraudsters to proliferate. The UK Financial Ombudsman suggests there are 3 main complaints they witness due to fraud:

1. **Unauthorised plastic card transactions that customer didn't make or authorise**
2. **Scams - where a customer is tricked into handing over their bank details, allowing a fraudster to take money from their account without consent**
3. **Scams where the customer was tricked into transferring money to the fraudsters account - often because they believed they were making a payment to their bank or another trusted organisation**

The biggest challenges face that of an anti-fraud unit, where all aspects of conduct must be clear, concise and in alignment with regulatory requirements as well as having both the firm and the affected client's best interests at the forefront. They essentially need to ensure 100% accuracy, efficiency, and effectiveness whereas the criminal only needs to get it right once.

The siloed nature of large banking enterprises and approaches unifying people, process and technologies has dramatically inhibited the ability to identify and respond to fraud risk and the ongoing detection of future risks. Typically, the role of data requires a complete rethink for the new digital fraudulent risks identified, often needing a 'back-to-basics' approach in alignment to new threats; one, to identify the weakness in the current approaches; and two, to set out new data structures which can support both the need for real-time threat identification, and offline investigations.

The evolution of technologies such as cloud-based platforms, graph networks and digital twin approaches within finance ecosystems creates vast opportunity to build out high-performance data engineering and data science capabilities. This in turn enables significant advancements in machine learning approaches to detect, counteract and prevent fraud at near-real-time processing speeds. As the capabilities of the digital twin base machine learning increases, the ability of 'What-if' scenario evaluations cause an incremental speed of continuous improvement. This continuous feedback loop that subsequently drives improvement is ever changing the processes to remove/improve/secure value chains that adapts to the ever-changing fraud ecosystem.

At a holistic level, banks and financial services institutions need to review their present data and analytics maturity in the fraud space, and then review the following approaches to stay ahead of the fraud threat. Ensuring readiness to tackle the ever-changing challenge is of paramount importance.

Sopra Steria has and continues to identify and support its clients across a multitude of areas including:

Threat-Based

Fixed rules interpreted and applied to data as policy; these take the form of hard-coded rules determined by compliance and risk owners, targeting business areas of known vulnerability.

Evolution

The ongoing analysis of data and optimisation of rules based upon statistical analysis and it's integration into existing platforms, ways of working and cultures.

Predictive Measures

The use of Machine Learning, often combining the use of unsupervised and supervised learning techniques, furthermore an advanced understanding around feature engineering with data; to create multiple/layered models which evolve to support adaptable to the changing state of fraud detection.

Unified Adaptation

The ultimate data layer, combined with structured and unstructured data from across multiple business sources in the form of a 'data mesh', providing an adaptive fraud data landscape as opposed to a monolithic data landscape which reduces business agility.

Each step realises significant value for any enterprise, but equally re-directs from a reactive, siloed organisation to a proactive, adaptable and agile organisation and thus requires vision and ownership to take a pragmatic view of the transformational steps needed and define a clear pathway forward.

So where should financial services organisations focus their data and analytics efforts to combat fraud?

Significant advances in the field of parallel process ecosystems using Graphics Processing Units (GPU's) now empowers banks and financial services institutions to adapt their models quicker in order to counteract the fraud schemes and attacks. The growth and expansion of MLOps methodology with a focus upon the continuous lifecycle of models and reusability, furthermore, tied to a greater model of working between data scientists and application developers has vastly changed the ecosystem of tools being used and cross-functional collaboration needed to combat fraud head on, driving the opportunity to act.

Complementing this, the improvements in the field of graph network are now expanding insights across areas of fraud detection which in turn supports the discovery of patterns and relationships between fraud activities and transactions processing that was not previously visible to the bank. This graph network of insights, coupled to the legacy fraud intelligence now supports feature engineering for high-performance machine learning methodologies that can adapt to the everchanging attack vectors of the fraud space.

More broadly, there is the recognised need for technology companies with the subject matter expertise from banks, policing, charities, research groups, and policymakers to generate an ecosystem of cooperation. Driving a clearer understanding of the fraud landscape and the type of responses required. This is endorsed by such regulators as the FCA who wish for greater interaction between relevant parties to ensure the response to fraud is a UK-wide response.

The evolution of process analytics is also enabling banks to map their business process quicker and more effectively. Such enhanced insights into the current state of the processes empowers the banks to generate a digital twin of their fraud processing capabilities. This digital twin supports a virtual ecosystem where new processes can simulate and test new novel concepts, enabling a quicker evolution inlife cycle of the fraud capability. Empowering effective and efficient machine learning generates a continuous improvement of the analytics capability that will accelerate in the future.

Combining advanced analytics and data engineering with the processing power of a **Robotic Process Automation (RPA)** tools ensures the ability to detect a fraud attack and mobilise a set of automated processes to counteract the fraud. These RPA agents can perform a specific check within the fraud business with repeatable effectiveness and efficiency. Such a capability empowers the banks to respond to fraud activities with scale and precision, creating a unified and consistent outcome.

So where should financial services organisations start?

The Data mesh is an up-and-coming paradigm that helps fraud teams quickly address pain points associated with other modern data platform approaches. The concept of moving fraud detection closer to the edge of the data solution is a new way of thinking and organising the processing.

The distributed data mesh enables hyper-scaling of the processes without generating a single data warehouse to cover multiple data areas in a distributed manner.The current models are now replaced with well-honed models that use a "golden thread" of the business data and processes to deploy a value-chain of ensemble models to adapt to the ecosystem in atomic shifts to counteract new attack vectors. This microservices based risk scoring enables a more granular response to the fraud ecosystem.

Prior rigid models are not coping with exponential increase of more customer and transaction data which is now flowing through their systems. The financial pressures on small merchants that are now forced by contactless card payments superseding cash as the dominant payment means are forcing these merchants into a fraud risk space they are not equipped to handle in the same manner as bigger merchants that have dedicated fraud departments. The system needs to adapt.

On the other side, banks must now together form alliances and partnerships to generate a unified and adapting ecosystem of anti-fraud capability. This capability should start at the edge with a point-of-sale terminal; flow through the complete process, and include criminal evidence gathering to ensure the police and courts can remove the fraudsters by higher prosecution rates. Sopra-Steria is a provider of banking software, analytics consulting to support our merchant, banking and policing clients in a single processing workflow.

Our Rapid Data Factory is a distributed processing engine that Sopra-Steria uses to process hyper-scale data mesh structures. The factory enables a processing methodology that can evolve and improve continuously to adapt to fraud demands within the ecosystem.

With the rapid shift of customers to digital banking channels and movement of fraud in the same direction, how existing data and analytics solutions and strategies are deployed require a significant rethink. Furthermore, the very processes which bond how people, process and technology are harnessed to combat fraud must be reimagined.

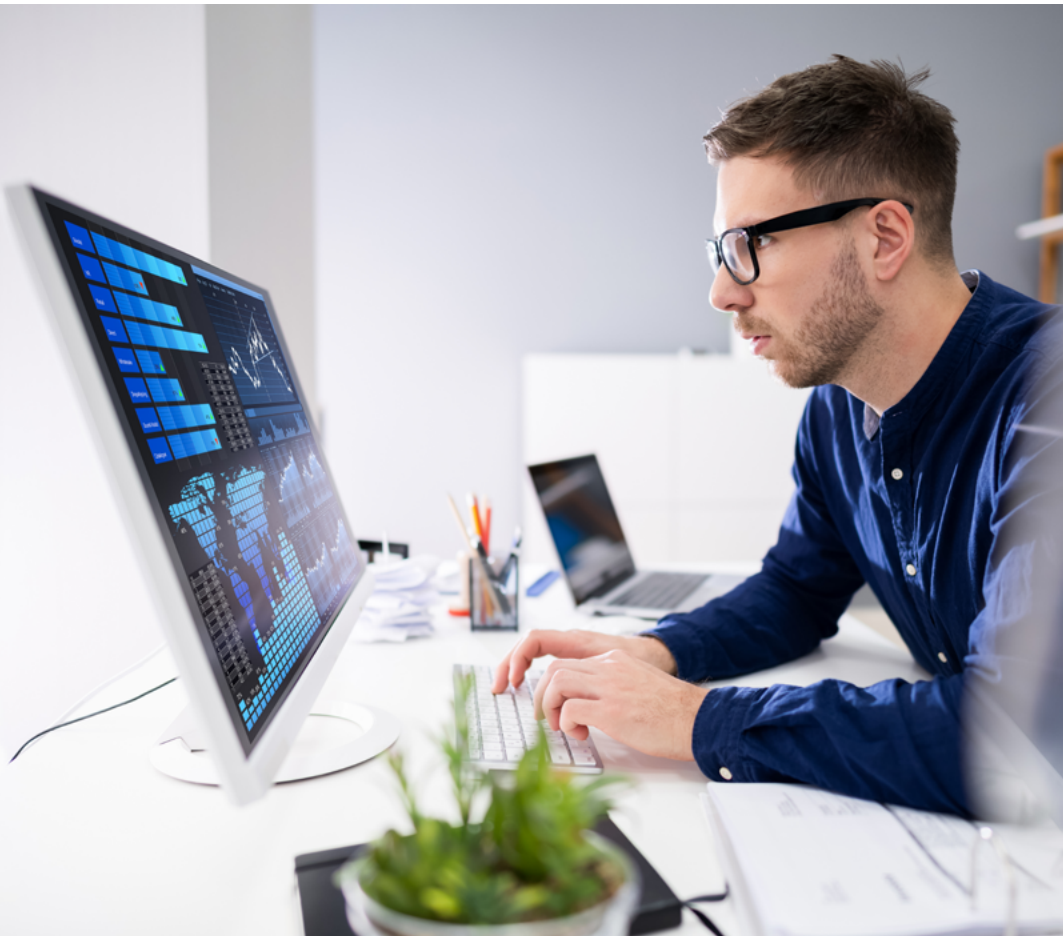
To this point, banks are now looking to approaches such as Process Mining as a central means to evaluate existing internal processes, identify internal 'friction points' and redefine and optimise processes. Such systems integrate across multiple data sources and can map out, for example the end-to-end fraud investigation process and consequently enable banks to clearly identify process bottlenecks and make appropriate impactful changes which can easily be quantified.

Leveraging process mining empowers banks and fraud teams to test through new processes and approaches and then apply ML, AI and RPA into the right areas where business value can be generated; identifying and improving existing processes and placing the spotlight on inadequate internal processes which were limiting the agility to face up to fraud challenges. Such approaches therefore improve visibility and accountability, demonstrating fraud teams understand the scale of change needed and have clear action plans in place.

The next-gen fraud system must support fraud prevention and the use of advance analytics methodologies as a minimum. The strategic move to a National Digital Twin for banking will in the near-future open opportunities for regulators to enforce regulations with the help of analytics and automation of processes. Regulatory scrutiny around fraud controls and the standards applied will inevitably increase; **Nikhil Rathi, the new CEO of the FCA makes it clear in the most recent 2021/22 Business Plan that the FCA will take a far more proactive and interventional stance on fraud (Chapter 5, page 28), with 'prevention' and 'disruption' sought by the regulator.**

Ultimately what is outlined here is a more assertive approach to fraud and the controls coming into practice, with clearer standards progressively being set in place. Although previous approaches, such as the banks stating what fraud controls they have in place and where on the FCA website, was considered a sufficient barometer of compliance.

It is now clear there will be a firmer focus upon the 'how' fraud will be managed, and banks who adopt an approach to focus on the very minimum standards, may witness more regulatory intervention. It is essential that banks and their fraud teams not only account for their internal anti-fraud strategies, but also remain mindful of the increasing expectation around standards being set by the regulator.



When should financial services organisations act?

Anticipating the shift to digital channels and the impact of this on fraud is something banks need to have a clear plan for now.

The change has also amplified the velocity and variety of data a bank now has, and therefore the ability to leverage this data to identify the risks early on is a space which is rapidly maturing. Strategies around Customer Due Diligence or **Know Your Customer ("KYC")** are one example of a key theme changing to adapt. Initially periodic reviews of customers based upon risk were the norm, with high leads times attached to remediation activities. It is now expected that perpetual KYC operations will gradually succeed, with the bar being set by regulators increasing, and thus it is logical to determine that internal improvements in a bank's own KYC people, processes and technologies will be subject to increased demand and scrutiny.

Again, only the minimum level of effort will not be viewed as sufficient by regulatory bodies. KYC approaches had been traditionally viewed as compliance-based, back-office activities, rather than an outcome which can materially benefit the end customer. This has all changed with the shift to digital services by customers. Those banks who are already cloud-based and have already transformed have now shaped their whole front-end ecosystem to work with a KYC-first framework, and therefore assess and determine risks far earlier in the engagement journey. They have turned the experience to their advantage, and as such have leveraged technological advances around KYC to lower the friction of digital experiences; provide a significantly improved customer experience; but have still managed to meet their risk appetite without significant compromise all round.

Banks must take an enterprise-wide approach to anti-fraud analytics - as we've touched upon earlier, fraudsters are becoming far more sophisticated in their approaches, using technology to their own advantage to evade detection. The over-reliance upon legacy fraud detection solutions has inevitably meant that banks have placed their trust in such wide-ranging solutions, however in parallel the fragmented landscape of solutions has progressively become an obstacle - presenting rigid foundations, when the common purpose now is to have both data and analytics at your fingertips to make faster and more assertive decisions.

Financial institutions need to get back to basics and ultimately ask themselves what the real problems with fraud are again, and not see the technology as the end-state solution. Cross functional collaboration, driven by a team mandated to establish both new thinking around fraud, and possessing the drive to challenge traditional ways is key to breaking down legacy business silo's and lead the way in how best to optimally tackle fraud. This requires a vision to see beyond the current people, process and technological challenges and understand how and where to bring in new data assets, diagnostic and predictive methodologies and determine a clear path which drives significant business improvement.

The vision equally cannot fall on the shoulders of a single business 'change-agent', to achieve success senior executives must learn to accept that we are in a time of considerable change and therefore remain open minded and supportive of a more collaborative approach to placing analytics at the heart of fraud management.

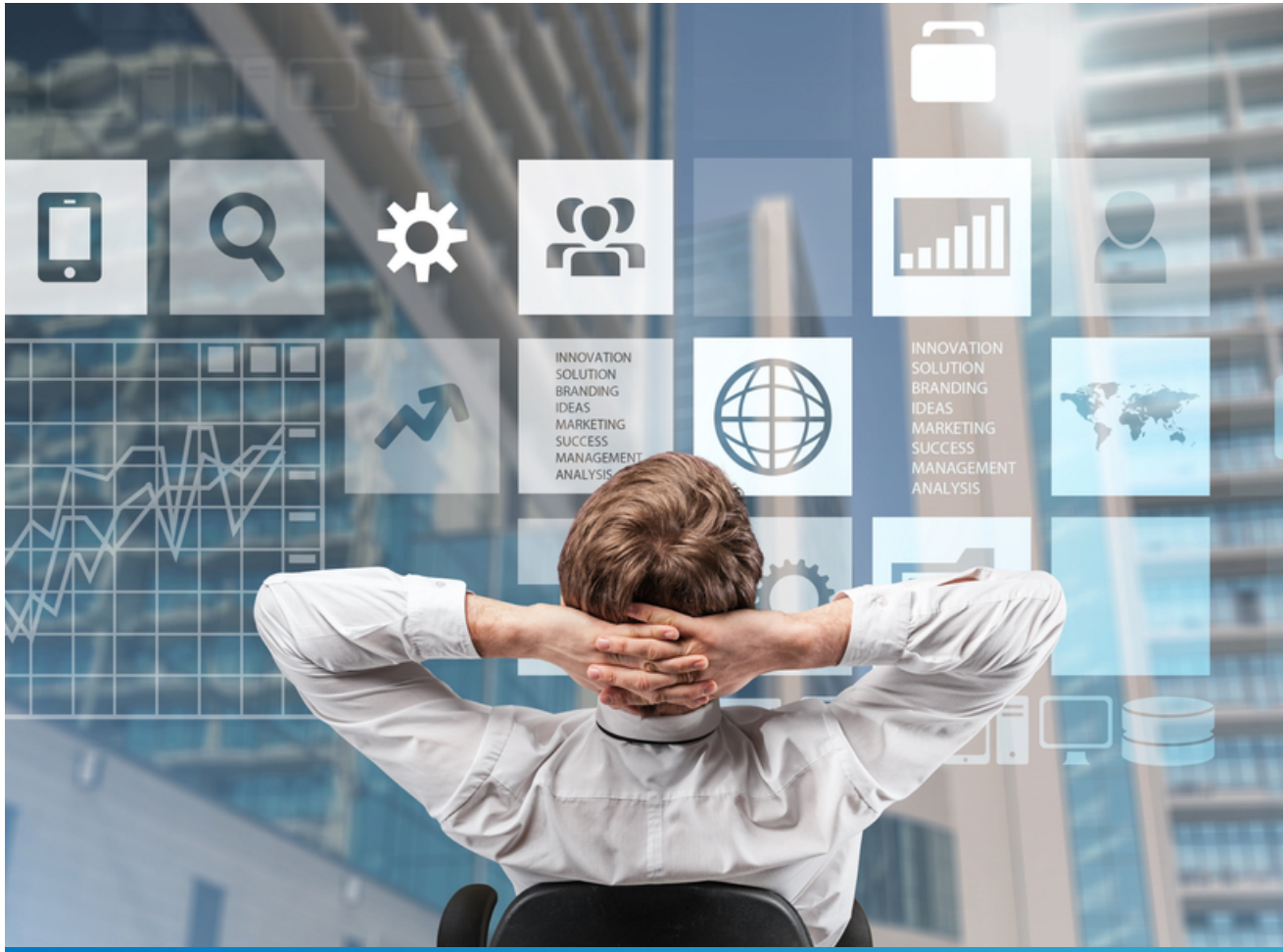
Data and Analytics teams need to act now not just from the bank's perspective but also from a criminal's perspective as well. By starting with what the criminal wants to achieve and how they plan to execute their plans data and analytics teams can create data driven insights and predictive modelling techniques which may highlight fraudulent behaviour before it really happens.

The creation of a digital twin of banking processes provides a trustworthy abstraction of information from multiple key systems which can then be used to not only identify but stress-test specific fraud vulnerabilities. For example, using Generative Adversarial Networks (GAN) against a virtual twin can be used to test anti-fraud models, ensuring that the adversary does not achieve fraud success.

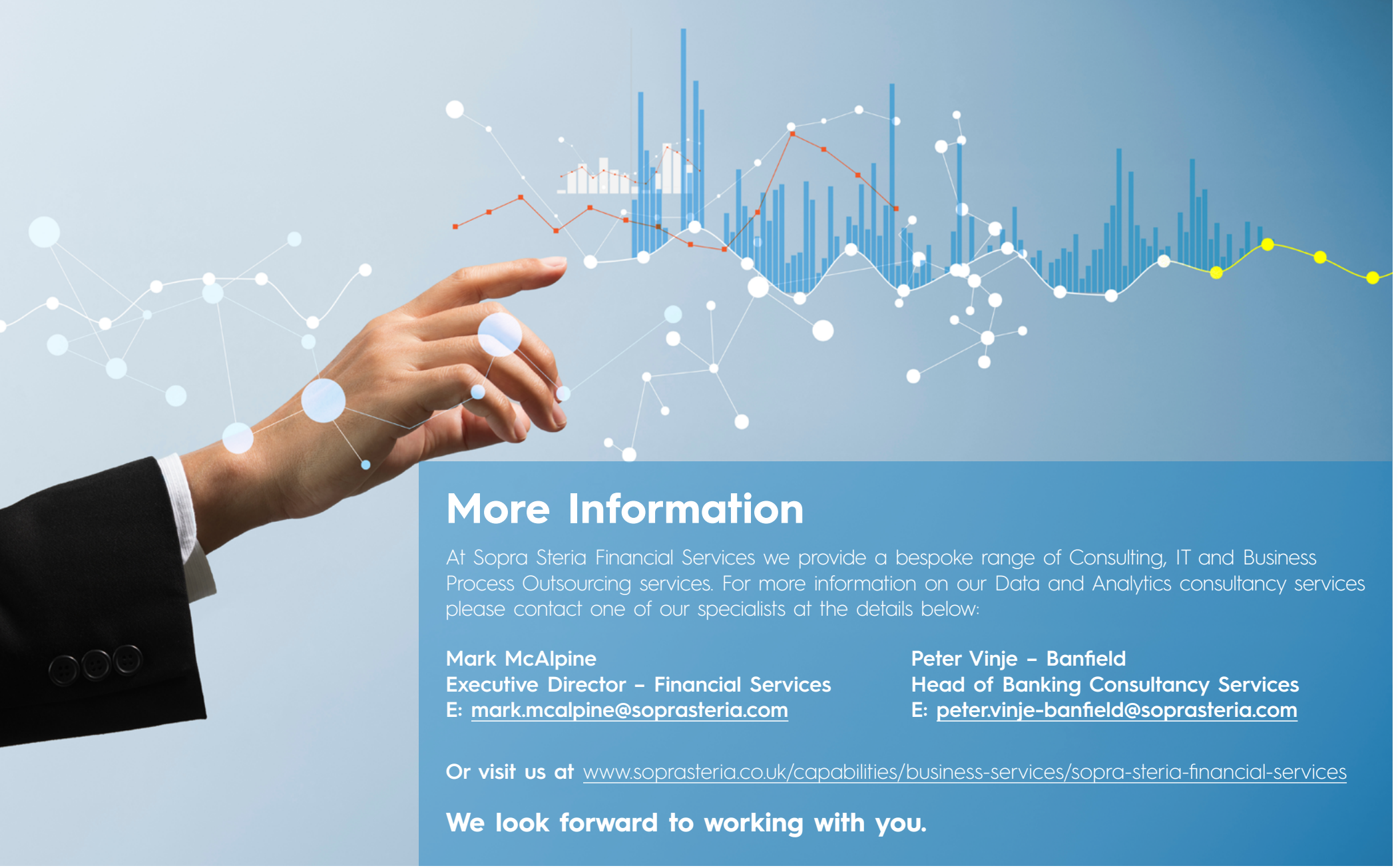
This accelerated reinforcement learning ecosystem enables the rapid detection and correction of attack vectors, presenting a unified view of fraud incidents and ability to evaluate any new changes against the known generative adversarial network attack vectors before opening the process to the customer base. This process mitigates the risks before they could happen.

Probably the most important and yet the most typically challenging aspect for a fraud team is to take a 'Customer first' mindset – and so visualise counter measures to fraud in harmony with the customer experience team. Analytics plays a crucial role in facilitating low-risk customers and transactions as they do in stopping potential fraud, enabling banks to create custom, analytics-informed journeys. Models must be built on the proper foundations, integrating customer behaviours across accounts and transactions into a single view that enhances the power of prediction and detection, but also doesn't present an onerous, overbearing experience for end customers.

Significant changes such as the higher shop floor limits for contactless payments will push further anti-fraud outcomes onto banks soon, in addition to the continuing risks being presented from the significant increase to online purchases. Therefore, the design of all future fraud models and teams alike must bridge a complex world which possesses, agility, accuracy and ethical considerations at its core.



Sopra Steria; a European leader in consulting, digital services, and software development, is helping its clients drive their digital transformation to obtain tangible and sustainable benefits in the business ecosystem of fraud. Our specialist Financial Services division and SME consulting capabilities ensure market-leading experience, skill-sets and knowledge across all aspects of fraud in order to empower our clients with fit for purpose strategies support by a foundation of data and analytical capabilities in order to drive effective and efficiency outputs.



More Information

At Sopra Steria Financial Services we provide a bespoke range of Consulting, IT and Business Process Outsourcing services. For more information on our Data and Analytics consultancy services please contact one of our specialists at the details below:

Mark McAlpine
Executive Director – Financial Services
E: mark.mcalpine@soprasteria.com

Peter Vinje – Banfield
Head of Banking Consultancy Services
E: peter.vinje-banfield@soprasteria.com

Or visit us at www.soprasteria.co.uk/capabilities/business-services/sopra-steria-financial-services

We look forward to working with you.

The world is how we shape it

sopra steria