FStech

# RegTech Live

## CONFERENCE OVERVIEW

## 27 February 2024

## London Hilton Tower Bridge

**Follow the event on X: @FStechnology #RegTechLive**

**Sponsored by**

InterSystems Creative data technology

PURESTORAGE Uncomplicate Data Storage, Forever

riskonnect.

smarsh

SmartSearch///

**Brought to you by**

FStech

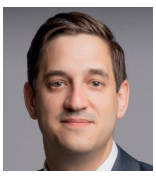
# RegTech Live

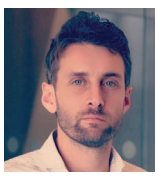
## CONTENTS














# INTRODUCTION

**Jonathan Easton,**
**Editor, FStech**

Welcome to FStech's RegTech Live 2024 overview.

Returning for its sixth year in 2024, RegTech Live this year brought data to the fore – whether that was providing insights on testing and recovery strategies or getting ready for regulations like DORA – and asked what financial institutions can do to stay ahead of the compliance curve at a time of continued political and macro-economic uncertainty.

The conference also took a close look at one of the most pressing topics of today: artificial intelligence (AI), with the impact of the technology being felt across the entire day. This ranged from a look at the convergence of communications data and machine intelligence to transform compliance, to what financial institutions can do to develop resilience against weaponised AI attacks.

The conference also featured a number of excellent presentations, including thought-provoking keynotes from Kate Fitzgerald, head of policy, Payment Systems Regulator on the topics of Open Banking and APP Fraud, and Nathalie Lowe, the Financial Conduct Authority's accountable executive for transforming data collection, who explored emerging technologies amidst evolving regulation.

Before wrapping up this introduction, I want to provide a special thanks to RegTech Live 2024's sponsors: InterSystems, Pure Storage, Riskonnect, Smarsh, and SmartSearch.

We are very thankful to everyone who attended and continues to support our events and awards, and I look forward to welcoming you to our next must-attend conference – The Future of FinTech, taking place at the Hilton London, Tower Bridge on 13 June 2024.

# RegTech Live

## AGENDA

**08.30 - 09.05: Registration and refreshments**

**09.05 - 09.10: Chairman's welcome**
Jonathan Easton, Editor, FStech

**09.10 - 09.40: Keynote speaker - Making sure payments are working well for everyone**
Kate Fitzgerald, Head of Policy, Payment Systems Regulator

**09.40 - 10.10: Getting your data regulation ready**
Joe Lichtenberg, Global Head of Product and Industry Marketing, InterSystems

**10:10 - 10.40: Panel - Exploring DORA: The landmark regulation's impact on financial services** *- sponsored by Riskonnect*
Panellists:
Alex Coleman, Global Chief Architect for Risk and Compliance, HSBC
Daniel McCatty, Principal for Cyber and Third-Party Risk, UK Finance
Sam Reason, Head of Operational Resilience and Continuity (inc Third Party Assurance/Governance), Zurich Insurance

**10.40 - 11.10: Coffee break**

**11.10 - 11.40: Operational resilience in financial services: Data, testing, and recovery strategies**
Patrick Smith, EMEA Field CTO, Pure Storage

**11.40 - 12.10: The financial cybercrime pandemic: Developing resilience against weaponised AI attacks**
Philip Treleaven, Professor of Computing, UCL, Director, UK Centre for Financial Computing

**12:10 - 12.40: Panel - The AI revolution: The convergence of communications data and machine intelligence to transform compliance** - *sponsored by Smarsh*
Panellists:
Fatima Abukar, Data, Algorithms and AI Ethics Lead, Financial Conduct Authority (FCA)
Shaun Hurst, Principal Regulatory Advisor, Smarsh
Dizem Ozalp-Sari, Head of Data Services, BNP Paribas
Andy Thornley, Head of Financial Services, techUK

**12.40 - 13.10: From Open Banking to Open Finance**
Andy Millar, Head of Strategy & External Engagement, Global Open Banking, HSBC

**13.10 - 14.10: Lunch break**

**14.10 - 14.40: Panel - Fighting FinCrime: How FSIs are using technology to simplify financial crime compliance** *- sponsored by SmartSearch*
Panellists:
Gareth Brett, Financial Crime & Risk Specialist
Zowie Lees-Howell, VP of Enterprise Sales, SmartSearch
Andranik Mnatsakanyan, Director, Visa Consulting & Analytics
Riccardo Tordera-Ricchi, Head of Policy & Government Relations, The Payments Association

**14.40 - 15.10: Keynote - Cracking the Code: Harnessing Innovation in the Era of Evolving Regulations**
Nathalie Lowe, Accountable Executive for Transforming Data Collection, Financial Conduct Authority (FCA)

**15.10 - 15.15: Chairman's closing remarks and end of the conference**

**15.15 - 16.15: Networking drinks reception**

# Keynote - Payment Systems Regulator

## Making sure payments are working well for everyone

**In this keynote presentation, Kate Fitzgerald, head of policy at the Payment Systems Regulator (PSR) provided insight into key areas the regulator is working on in this fast-paced, ever-changing industry. The session focused on examining how to unlock Open Banking for more users and explored APP scams from a user protection perspective.**

"Better competition between payment systems can lead to better outcomes for users, more innovation, and better-quality solutions," said Fitzgerald.

She told delegates that the need for innovation in payments is clear, adding that it is necessary in order to improve the industry and make sure users are better protected.

Fitzgerald talked about how the phenomenon of Open Banking can give more granular control to how and when consumers pay their bills. However, she warned that to be beneficial on a wider scale, it needs to be adopted by a large part of the industry.

"It's not enough for just one or two banks to join," she said. "This is where regulation can help."

Fitzgerald continued: "More work needs to be done on how to deliver a commercial model that encourages competition and adoption – it's a key trade off. How do you price Open Banking payments that offer great value to merchants but also drive adoption, and encourage banks and others to join?"

Next, the head of policy spoke about the upcoming mandatory reimbursement scheme for APP fraud, which is being introduced by the PSR later this year. She explained that the move aims to drive consistency, trust, and incentives to tackle fraud so that customers can enjoy a minimum level of protection.

"It's a strong incentive for payment firms to do better when it comes to fraud protection because the more they do the smaller their bill for reimbursement is," she said.

Talking about the risks of generative AI being used to carry out APP fraud, Fitzgerald said that the ability for fraudsters to manipulate people is already "really strong".

"APP is growing and it's probably under reported," she told delegates. "With the growth of new tools there is more of a threat, that's why we actually need payment firms to step up and protect customers."

She added: "This is where we think the payment firms need to get ahead and identify malicious actors. We really need innovation to power ahead."

Touching again on Open Banking, Fitzgerald said that investment has grown, with a wealth of FinTechs jumping into the space and a lot of new innovation happening.

However, she said that it is still limited at the moment. For example, she explained, it currently doesn't provide a real replacement for other forms of payment because you can't use it in a shop or to pay a bill, and it's rarely available for e-commerce.

"In this country it's very dominated by Visa and Mastercard and competition could really help inject innovation if we had another way of making payments," she said. "That's really our ambition."

## InterSystems

# Getting your data regulation ready

**In this session Joe Lichtenberg, global head of product and industry marketing at InterSystems, explored how financial services providers (FSIs) can get their data regulation ready.**

While timely responsiveness to regulation is imperative to avoid fines and reputational risk, Lichtenberg referred to a survey from InterSystems which found that 56 per cent of firms struggle to maintain data consistency and usability when it comes to compliance. He explained that this is often driven by the fact that many processes are still manual, which means firms are hampering their ability to meet regulatory mandates like the Consumer Duty.

He told delegates that getting data into a usable format is still really difficult, adding that managing risk can be complex with many internal and external data points.

Lichtenberg added that with lots of disparate data sources, firms are often dealing with a "data explosion".

When it comes to the Consumer Duty, he explained, to make sure products and services are up to scratch there needs to be a 360-degree view of customers. He added that it is particularly important for vulnerable customers to get fair value.

"You need to identify how your products compare from a value and price standpoint," he said. "You need to pull in external data and this can be complex."

Lichtenberg added that there needs to be a continuous monitoring of consumers and that firms need to drill into raw data and have a centralised metadata layer to support overarching governance.

"All of this is really a big data problem," he said.

But he continued on to say that there are methods in the market that can help to address some of these key issues. He said that analysts are now promoting an exciting new approach to help FSIs eliminate data errors: data fabric.

Lichtenberg explained to delegates the many ways that this type of infrastructure can address the challenges around data sprawl, latency, and being able to ask ad-hoc questions of the data a company collects.

# Panel – sponsored by Riskonnect

## Exploring DORA: The landmark regulation's impact on financial services - sponsored by Riskonnect

**The Digital Operational Resilience Act (DORA) is a landmark piece of legislation that aims to strengthen the operational resilience of financial institutions in the European Union. In this session, expert speakers discussed DORA and its implications for RegTech, whilst also examining what financial institutions should look for in solutions to address the requirements of the game changing regulation.**

Daniel McCatty, principal for cyber and third-party risk at UK Finance, said that the time frame for the Act was "very, very ambitious".

"There's only one year until everyone needs to be compliant, I'd be surprised if anyone in this room was to say they are definitely on target," continued McCatty.

Sam Reason, head of operational resilience and continuity (incl third party assurance/governance) at Zurich Insurance, said that the shorter time frame is likely attached to the probability of a disruptive incident happening.

"To be fully compliant by then will be a challenge," added Reason. "It's more about a flight path to compliance; if we're not compliant, what actions do we need to address to get there?"

Discussing the key cultural and organisational changes firms need to truly embed resilience, Alex Coleman, global chief architect for risk and compliance at HSBC, said that because there is currently a "patchwork quilt of regulation" it is necessary to introduce an end-to-end framework.

Coleman further explained the importance of identifying how to turn purely tech-related conversations into customer outcomes.

Zurich Insurance's Sam Reason said that he has often in the past seen a culture whereby the head of IT is expected to be solely responsible for operational resilience. He agreed with Coleman that companies need to focus on the end customer, which is often not the same as the IT customer.

Daniel McCatty from UK Finance went on to say that when it comes to operational resilience, for many firms, the fact that a direct return isn't a quick process is a "hard pill to swallow".

HSBC's Alex Coleman highlighted the importance of joining up the data across an organisation.

"In particular, DORA drives us to think about the interrelationship between the data, taxonomy, risk management, and resilience, and use it to prioritise decisions and focus," he told delegates.

Speaking about the role of scenario testing, crisis simulation exercises and table-top drills, Coleman said that these exercises give a better view of the threats faced by financial services providers and the likelihood of them happening.

"All of that gives us a richer picture to that conversation, where do we focus our efforts and minimise the impact?" said the global chief architect. "How do we quantify the likelihood and the urgency behind mitigating some of those urgencies?"

## Pure storage

# Operational resilience in financial services: Data, testing, and recovery strategies

**Financial services firms face a complex and evolving threat landscape that makes operational resilience more important than ever. New regulations such as DORA are raising the bar for operational resilience, requiring firms to identify their most important business services, and set impact tolerances. Robust data and testing will only become more key to meeting these new requirements as threats continue to evolve.**

With the advent of DORA, Patrick Smith, EMEA Field chief technology officer, Pure Storage told attendees that the meaning of operational resilience around data is evolving at pace.

"Operational resilience now means that ICT is a huge area of focus for every organisation," he said.

In this effort, Smith explained that it has grown essential for organisations to understand how critical business services, the applications supporting them, along with the technology supporting those applications, all join together.

"Planning is essential, not just for organisations to understand how, but also to evidence to the regulator how they can recover from a worst-case scenario and meet the requirements of DORA," he said.

Smith went on to note that cybercrime has dramatically changed the threat landscape because it circumvents a lot of the protections and controls for an organisation which were previously sufficient.

"The perimeter controls around stopping an attack in the first place is the number one goal, but if an organisation can't do that, making sure they can properly react to a worst-case scenario is absolutely essential and there is no one-size-fits-all approach to protecting data," he said.

In data protection, Smith instead advised a move away from a one-size-fits-all approach to business application and data security.

"Instead, we need fitness-for-purpose and fitness-for-priority, meaning that organisations need to evaluate on a more individualist basis the technology, procedures, policies and plans organisations have in place that take them all the way from Tier 0 apps towards other less critical areas of their data stack," he concluded.

## UCL

# The financial cybercrime pandemic: Developing resilience against weaponised AI attacks

**With losses to cybercrime rising to an estimated $27 billion in 2023, many financial institutions and regulators are ill prepared to deal with the emergence of new technologies being used by cybercriminals. We have already seen generative AI platforms and other new technologies start to 'industrialise' cybercrime within its own ecosystem, while the potential of Algorithmic Superintelligence (ASI) which far surpasses even the most gifted human minds should ring alarms for banks and regulators alike.**

Philip Treleaven, director of the UK Centre for Financial Computing and professor of computing at UCL opened his talk by stating that innovation in technology over the coming years will largely be driven by cybercrime.

As technology evolves, Treleaven pointed out that while cybercriminals are evolving their tactics, using ChatGPT to write criminal programs and other data science techniques to gain an advantage, cybercrime is also becoming more industrialised.

"Nowadays financial institutions are not just up against lone bad actors working out of their bedroom, but rather criminal syndicates who may even be working in collaboration with rogue states like North Korea," he said.

With more sophisticated criminals and the rise of industrialised cybercrime, Treleavan stressed the importance of real time threat detection.

"You've got to do real time detection because if you think of something like the Digital Operational Resilience Act (DORA), it's been about five years in the making, but these innovations coming from cybercrime need to be tracked in real time," he said.

Treleaven moved on to reflect how advances in technology are rendering security protocols that once worked well enough, more tenuous.

"Nowadays if you record just a three-second conversation with someone, you can completely replicate their speech and get them to say anything you like," he said. "The digital banking mantra of 'my voice is my password' is now absolutely shot."

Looking ahead, Treleaven said the continuing evolution of the digital future, with the rise potential of Algorithmic Superintelligence (ASI) – so-called superintelligent algorithms that can do "anything better than humans" – digital avatars for virtual spaces like the metaverse, along with criminals' algorithms and malicious programs running out of computers situated across multiple jurisdictions, are all likely to causes even more challenges.

"It's an exploding universe and the big problem is a case of simply understanding all of these different areas and the emerging technologies," Treleaven said, but noted that it's likely that the biggest challenge around evolving cybercrime will be related to jurisdictions. "If you have a computer that does insider dealing or something, they are going to be in a specific jurisdiction, and the challenge with cybercrime will be in regulating it when it is emanating out of places like North Korea which don't have legislation in place."

## Panel – sponsored by Smarsh

# The AI revolution: The convergence of communications data and machine intelligence to transform compliance - sponsored by Smarsh

**The ability for Artificial Intelligence (AI) and Machine Learning (ML) to process and analyse large swathes of data presents a revolutionary means of maintaining oversight of electronic communications. New technologies like generative AI (GenAI) and large language models (LLMs) are also opening new ways for financial institutions to transform compliance in this area.**

In this session, expert speakers discussed why and how financial institutions are converging AI and ML technology with communications data to evolve their compliance strategy, and how financial institutions can leverage that data to quickly identify and minimise risks, illuminate new business opportunities, and improve operational systems.

The panellists began by exploring some of the biggest challenges financial institutions face in implementing AI for compliance functions.

Fatima Abukar, data, algorithms and AI ethics lead at the Financial Conduct Authority (FCA), talked about the challenges linked to integrating AI into an infrastructure that relies on legacy technology. An additional challenge, she explained, is the dependence on third-party organisations.

"It's important to touch on the governance of AI," continued Abukar. "How do we collect and analyse data using AI technology whilst deploying it securely?"

Shaun Hurst, principal regulatory advisor at Smarsh, said that one key challenge is how quickly the space is moving.

"People are getting stuck because there are so many exciting things happening," he continued. "There's no best time to do it."

Dizem Ozalp-Sari, head of data services at BNP Paribas, said that it can be a challenge because in financial services organisations are operating in a live system.

"Sometimes it's difficult to identify where the benefit of implementing the AI is," she said. "Many financial services providers are having difficulty finding the right profile for the right technology. They're trying to recruit for a particular technology but haven't figured out how to match the regulation."

Speaking about how financial services providers can ensure AI compliance solutions meet regulatory expectations around explainability, fairness, and human oversight, the FCA's Fatima Abukar said that firms should consider who is responsible and identify where the risk management of AI sits within an organisation.

Andy Thornley, head of financial services at techUK, said that responsibility shouldn't lie with just one person.

"Our members are saying that when you have one individual, it means there can be an overly cautious approach which can stifle innovation," explained Thornley.

Smarsh's Shaun Hurst, said that one key concern brought up with customers is job losses.

"GenAI is creating content, and it still needs to go through compliance, so it's actually creating even more work," he explained to delegates.

Hurst went on to say that a guided, robust training model is necessary.

"Don't be scared of what's coming, learn about what's coming," he concluded.

# HSBC

## From Open Banking to Open Finance

**The Data Protection and Digital Innovation Bill (DPDI) is expected to pave the way to Open Finance in the UK. The European Commission has published its Financial Data Access (FiDA) draft proposal which will enable Open Finance in the EU bloc. What does this mean, how ready are we, and what do we need to do to bring Open Finance to reality for our customers?**

These are the questions Andy Millar, head of strategy & external engagement, global Open Banking, HSBC attempted to answer in his session. He opened his speech by stating it had taken HSBC six years to reach a good standard of scale in Open Finance and will likely take another six years to establish itself across other areas of banking.

Millar explained that a lot of the most time-consuming elements of Open Finance relate to how security protocols are going to be made to work.

"Most aspects can't yet be done in full because we don't have all the data available," he continued. "We can't yet, for instance, share data with insurance companies."

Millar explained that on a global level, another challenge to the rollout of Open Banking is that each market operates differently. "The UAE, for example, has set out a whole profile for financial services and Open Finance, and it's emanating from its central bank rather than payment or data legislation," he said. "In their thinking, they seem to be listing out customer use cases then backward working to understand what technology and data they need to make things work, instead of first making people share data and then hope relevant use cases come along."

Millar moved on to the most important considerations around Open Finance.

"Security trust is a key consideration, no more so than with third parties accessing your data," he said. "If that comes down, the entire concept of Open Finance breaks down."

He added that the customer has to trust it, but respective infrastructures that make Open Finance possible also have to be able to trust one another.

Another key challenge around the evolution of Open Banking is around liability, explained Millar.

"The reason cards are so successful is because if there's card fraud, customers know they are protected," he said. "Open Banking doesn't have that same level of liability support and that's what needs to happen to get it to the next stage."

For the UK, Millar highlighted that a key challenge for Open Banking was that its financing is currently done by nine banks. "At the moment, there's no way forward on how we're going to finance the industry and how FinTechs are going to achieve it," he said. "I'm not talking small FinTechs, but the likes of Apple and Amazon using Open Banking, so you can't expect them to be subsidised by nine banks, and this is what needs to improve from an ecosystem point of view."

## Panel – sponsored by SmartSearch

# Fighting FinCrime: How FSIs are using technology to simplify financial crime compliance

**As regulation and compliance duties expand, financial institutions face increasing pressure to fulfil obligations efficiently and cost-effectively. In this session panellists explored how leading firms are turning to next generation RegTech to simplify know your customer (KYC), anti-money laundering (AML), and sanctions screening processes for efficient and cost-effective compliance. The experts also discussed the current RegTech landscape, including how leveraging data and technology strategically can optimise compliance productivity, and the transformative potential of automation through machine learning.**

Regarding current financial crime challenges for the coming year Riccardo Tordera-Ricchi, head of policy & government relations at The Payments Association highlighted the challenge for organisations to stay ahead of the curve.

"The cost of compliance, with a need for skills and tools you need to have to be on top of the market, is clearly one of the most important things at this time," he said.

Gareth Brett, financial crime & risk specialist saw a key compliance challenge for FSIs in coming to terms with huge volumes of data.

"Compliance costs for financial organisations are going to increase by orders of magnitude because AI is going to continue generating enormous amount of data," he said. "The challenge becomes one around how organisations are going to process this and perform effective transaction monitoring."

Zowie Lees-Howell, VP of enterprise sales, SmartSearch viewed a rising challenge around data access.

"There's a challenge around navigating access to the right data to make the right decisions and minimising risk while making sure the customer gets the right experience," she said. "Balancing all of that while ticking regulatory requirement boxes is quite a challenge."

The discussion moved on to emerging strategies and the technology showing most promise for 2024.

"Customers we talk to are focused on taking a more data-driven approach," said Lees-Howell. "In the past processes were heavily rules-based, but now there's a shift to data, and while challenges remain, the opportunities around tech like AI and ML are huge."

Tordera-Ricchi agreed about the potential of AI and its application to the lifecycle of the customer.

"Regarding techniques to prevent crime, how we're going to merge AI with existing security processes is going to be important," he said.

The panel went on to focus on the top considerations for balancing KYC considerations with compliance as onboarding becomes digitised.

"When we run an onboarding strategy, it's about educating customers about potential risks and potential fraud and compliance requirements," said Andranik Mnatsakanyan, director, Visa Consulting & Analytics. "We try to make sure that user experience is as simple as possible, in addition to making sure we are ticking all the boxes."

Tordera-Ricchi added that the customer-centric approach has proven to be the way forward.

"But I also think there's a further step to it which is a risk-based approach, wherein you cluster customers based on their data which helps create opportunities for different user journeys based on their needs," he concluded.

# Keynote – Financial Conduct Authority

## Cracking the Code: Harnessing Innovation in the Era of Evolving Regulations

**During this keynote speech, Nathalie Lowe, accountable executive for transforming data collection at the Financial Conduct Authority (FCA) explored the emerging technologies currently impacting the financial services industry and delved into the evolution of regulation.**

In this session, attendees also gained insights, inspiration, and actionable lessons, such as hearing about how the FCA uses technology and policy sprints as an innovative tool for regulation, as well as its work on sandboxes to assist innovation in the market.

Lowe began by highlighting that AI and regulation is a landscape marked by both challenges and responsibility. She spoke about how regulation is often a key driver of innovation, referring to how a host of new services and technologies were driven by regulation like GDPR.

"It's essential that a strong digital infrastructure is in place to support AI deployment," continued Lowe. "But how many regulators can we honestly say truly understand the AI deployment? The bulk of AI deployments are not only powered by large data sets but will also be run on the cloud. These cloud-based services and the interdependencies they create in the data sets result in third critical party risks."

She highlighted that if one of these critical third-party services were to be disrupted, the impact on financial services infrastructures could be "destabilising". This, Lowe explained, is why the FCA is currently developing an approach to addressing these risks.

"It's only with the resilient and well-functioning physical infrastructure in conjunction with high quality data that AI can make the most positive impact," she continued.

Lowe went on to say that privacy is a top concern, explaining that financial transactions are sensitive and the balance between utilising data for beneficial purposes and respecting individual privacy is important.

"Striking this balance requires robust regulatory frameworks on how individuals will have control over their data, while allowing for responsible use in the pursuit of innovation," she told delegates.

Next she spoke about some of the risks associated with the technology, like deepfakes, which she said can turn the "credible into the untrustworthy".

# RegTech Live

# SAVE THE DATE

## FEBRUARY 2025

Follow the event on X @FStechnology #RegTechLive