FStech Conferences

RegTech Live

CONFERENCE OVERVIEW

28 February 2023

London Hilton Tower Bridge

Follow the event on Twitter: @FStechnology #RegTechLive

Sponsored by

Camms. NICE Actimize novatus advisory riskonnect smarsh

Brought to you by

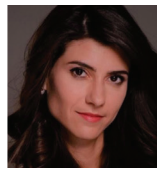
FStech

RegTech Live

CONTENTS



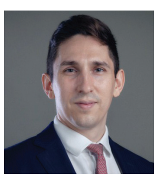














FStech Conferences

INTRODUCTION

Jonathan Easton,
Editor, FStech

Welcome to our RegTech Live 2023 overview.

Returning for its fifth year in 2023, RegTech Live took a look at the technology designed to help financial services firms maintain regulatory compliance in a rapidly changing risk landscape.

The day saw speakers discuss and explore how regulatory expectations are changing amidst a backdrop of macro-economic uncertainty and disruption, with a focus on key areas such as digital transformation, regulating financial innovations across crypto, DeFi, and block tokenisation and operational resilience.

Bookended between keynote speeches from senior figures from the Open Banking Implementation Entity (OBIE) and the Bank of England's Prudential Regulation Authority, we heard panellists discuss compliance, hybrid working, methods of tackling financial crime and the upcoming European Market Infrastructure Regulation (EMIR) Refit.

Before wrapping up this introduction, I want to provide a special thanks to our sponsors: Camms, Nice Actimize, Novatus Advisory, Riskonnect and Smarsh.

I hope you find this booklet to be a worthwhile complement to the conference itself, and we look forward to welcoming you to RegTech Live 2024 and the other conferences we run at FStech.

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: UK Open Banking regulation: How far have we come and where are we going?
Alan Ainsworth, Strategy, Policy & Standards Director, Open Banking Implementation Entity

09.40 - 10.10: The Journey to Risk Management Maturity
Daniel Kandola, Vice President, EMEA, Camms

10.10 - 10.50: Panel - When disaster strikes: how can financial services providers stay compliant in times of disruption? – *sponsored by Riskonnect*
Panellists:
Paul Cutler, Managing Consultant, Riskonnect
Emma Hagan, Chief Risk and Compliance Officer, ClearBank
Andrew Rogan, Director, Operational Resilience Digital Technology & Cyber, UK Finance
Adam Stage, Operational Resilience Senior Manager, TSB
Irina Velkova, Associate Director, Grant Thornton

10.50 - 11.30: Coffee break

11.30 - 12.00: An Evolution in Ongoing Monitoring: The route to greater effectiveness in transaction monitoring.
Adam McLaughlin, Global Head of AML Strategy and Marketing, SME, NICE Actimize

12.00 - 12.30: Regulating Financial Innovation
Philip Treleaven, Professor of Computing, UCL, Director, UK Centre for Financial Computing

12.30 - 13.00: Panel - Hybrid risk: meeting regulatory standards in an era of remote working and digital transformation – *sponsored by Smarsh*
Panellists:
Samaroha Das, Director of IT Risk, Metro Bank
Shaun Hurst, Principal Regulatory Advisor, Smarsh
Hannah Parvin, Manager, Deloitte Cyber Risk Service Practise
Sarah-Rose Perry, Head of Compliance, Octopus Investments

13.00 - 14.00: Lunch break

14.00 - 14.30: Fireside Chat – How can the industry collaborate more effectively to digitally optimise controls and meet regulators' expectations of more effective outcomes in fighting financial crime?
Richard Maton, Executive Director, International RegTech Association (IRTA)
Paul Munson, UK Director of Compliance, Shares

14.30 - 15.00: Panel - Ready to refit: RegTech's role in preparing FSIs for the EMIR Refit – *sponsored by Novatus Advisory*
Panellists:
Carolyn Jackson, Partner, Katten UK
John Kernan, Chief Executive, REGIS-TR
Hannah Meakin, Partner, Norton Rose Fulbright LLP
Matthew Ranson, Partner, Regulatory Advisory Practice and RegTech, Novatus Advisory

15.00 - 15.30: Keynote speaker: The PRA's work on RegTech and Data in 2023 and beyond
Lewis Webber, Head of RegTech, Data and Innovation, Prudential Regulation Authority, Bank of England

15.30 - 15.45: Chairman's closing remarks and end of the conference

15.45 – 16.45: Drinks reception.

Keynote – Open Banking Implementation Entity (OBIE)

UK Open Banking regulation: How far have we come and where are we going?

UK Open Banking has come a long way since 2018, with seven million active users thanks to a world-class regulatory structure and thriving ecosystem. In this opening keynote session, Alan Ainsworth, strategy, policy and standards director at the Open Banking Implementation Entity (OBIE) explored what the country's regulators, FinTechs, and financial institutions need to do to stay ahead as other nations leapfrog the UK in taking Open Banking technology further to Open Finance.

Ainsworth began by defining Open Banking, explaining that the concept is "not rocket science". Instead, he told delegates, it makes the process of paying for things from a bank account more simple than it might otherwise have been. The data involved in Open Banking also enables people to better manage their finances and makes it easier for "surplus funds to go further", he said.

"Open Banking is not about the technology, it's about making life easy," said Ainsworth, adding that consumers can now set up payments from current account providers automatically across the UK's nine largest banks.

He warned that while the UK has been relatively successful, if the country does not "push ahead", it could be left behind.

Ainsworth talked about how his organisation, which has been focussed on Open Banking implementation, has no equivalent in the EU.

"There's nothing to ensure things are working," he said, adding that it's no wonder some other countries have faced issues implementing Open Banking when there is no single standard.

However, he did say that current UK regulation "isn't perfect" because it's based on older legislation.

"There are a lot of data sets that don't fit into the regime," he added, explaining that the organisation finds that some transactions don't work, and banks often impose payment limits.

He continued: "There are a bunch of idiosyncrasies where some issues were not conceived of when the legislation was first put forward."

Ainsworth warned that the UK doesn't necessarily have the agile regulation needed to deal with some of these issues, adding that Open Banking has lots of different stakeholders because there are many different regulators involved.

He told delegates that he is optimistic about what the upcoming Data Protection and Digital Information Bill will do for Open Banking – adding that it would be an improvement for consumers to be able to deal with things like insurance without having to re-input information and have this already completed instead.

However, he told delegates that looking ahead "fixing the basics" is something that needs to happen. This would allow the industry to identify what is blocking some areas of Open Banking and highlight parts that are not working properly, such as lack of education around the concept.

Camms

The journey to a mature risk approach

In this session Daniel Kandola, vice president EMEA at Camms, talked about the different processes and approaches to managing risk. He said that it is important for companies to develop a mature approach to risk.

Kandola explained that there are certain things businesses can concentrate on improving to help them achieve this.

The first is culture: firms should ensure that the right culture is embedded to help inform strategy and decision making.

Secondly, companies need to look at their processes. Regulations should not merely be a compliance exercise and companies should ensure their processes are efficient and not fragmented across departments, he explained.

"Mature processes are refined, they work, they are not just copied from a playbook. They are well thought out and considered," Kandola said.

Companies need to make sure that they have experienced, qualified people leading the approach to risk management. Kandola said that these people can help with the application of processes and provide the right guidance to ensure that companies move from an immature approach to risk towards a more mature one.

He told delegates that while software can help companies with their risk management, it should not be seen as a one-stop solution.

"We believe that having the right technology in place will ultimately give you a head start into ensuring that your maturity continues to grow and evolve. But it's not the answer to everything and it's not going to resolve all of the processes that you need to put in place," Kandola said.

He added that companies which have been successful at mitigating risk have continued to evolve.

"They have continued to ensure that they are improving and refining their approach to risk and not just absorbing it. They are actually communicating risks across their stakeholders," he concluded.

Panel – sponsored by Riskonnect

When disaster strikes: how can financial services providers stay compliant in times of disruption?

As the financial industry faces an onslaught of disruption amidst a challenging socio-economic backdrop, operational resilience has never been more of a priority for supervisory bodies. And the regulators are clear that financial services providers must have robust plans in place to ensure they are ready to act when disaster strikes.

Firms must prepare for everything from IT systems outages, cyber-attacks, and third-party supplier failure, to natural disasters, the cost-of-living crisis and global pandemics, ensuring they stay compliant across different geographic and regulatory jurisdictions.

This panel session, featuring expert speakers, explored the challenges and opportunities for financial services providers as they navigate an increasingly disruptive environment. Panellists also took a closer look at the role of technology in ensuring they are meeting rules and regulations.

Adam Stage, operational resilience senior manager at TSB, said that when it comes to resilience, it's important to think about outcomes and look at it from a "horizontal service lens" rather than across vertical silos.

Andrew Rogan, director of operational resilience digital technology and cyber, UK Finance, said that when he first started working for the trade association, the type of failures the organisation saw were fairly diverse.

"For the customer, the cause of the disruption was less important than the impact," he told delegates, explaining that consumers don't care why something has broken, they just want it fixed as soon as possible.

Next panellists were asked if when a key business service fails and damages a company's reputation it matters to the key stakeholders – including the regulators – whether the failure of the process was categorised as Operational Resilience, Business Continuity Management, or IT Disaster Recovery.

"Ultimately, no," replied Emma Hagan, chief risk and compliance officer, ClearBank. "If you're out, you're out – fundamentally it's the outcome that really matters."

Paul Cutler, managing consultant at Riskonnect said that operational resilience is about the ability to adapt.

"There's no point in blaming anyone during the incident," he said, adding that it's important for organisations to adapt and learn as they go.

When asked about the biggest challenges being faced by FSIs when it comes to meeting operational resilience standards, Irina Velkova, associate director at Grant Thornton, said that the pandemic was one of the biggest tests to assess whether firms could effectively deploy crisis planning.

"The proof is in the pudding," she told delegates.

Velkova added that a holistic approach is needed, particularly when trying to identify how to manage operational resilience within a "massive global organisation" or when dealing with the fast pace of technology and innovation.

Riskonnect's Paul Cutler said that companies adapted well to the pandemic and made this type of disruption a "plausible scenario" for firms. He explained that it also forced firms to explore what should come first: protection or customer service?

Nice Actimize

Greater effectiveness in transaction monitoring

In this session Adam McLaughlin, global head of AML strategy and marketing, SME at NICE Actimize, talked about how financial institutions needed to adapt their transaction monitoring processes and technology to defend against ever increasing risks.

He said that transaction monitoring has evolved with the introduction of AI, ML and big data, yet the end goal is ultimately the same - to stop and spot suspicious behaviour.

McLaughlin explained that transaction monitoring (TM) should start with KYC. "If you don't know your customer, how can you assess them for risk? How can you monitor them for suspicious activity if you don't know what they are doing?" he said.

He added that data is "king" when it comes to understanding customers. FSIs should look at using third party data and segmenting their customers as better ways to understand them, he continued.

McLaughlin went on to say that while TM technology is fairly new, it can take away human error and go through the necessary processes much faster.

"What TM technology can do is look across all the customer segments, the wider customer base and see if there are any deviations. It will continue to learn and optimise the outcomes and keep improving," he said.

McLaughlin added that FSIs will get precise alerts to suspicious transactions if everything is working efficiently. If the information is accurate, FSIs will be able to get the right information to the right people at the right time, resulting in recovery rates rising, he told delegates.

He warned that while technology can help FSIs, it is "only as good as the people using it".

"Humans are a key part of the system," he concluded. "Software is not going to save the world, technology is not the silver bullet and never will be. You still need to have investigators; you still need people who know what they are doing and who can spot suspicious behaviour and make decision."

Professor Philip Treleaven, UCL

Regulating Financial Innovation

The increased adoption of social media, artificial intelligence, blockchain and quantum computing technologies poses huge challenges for financial regulators who strive to maintain a balance between fostering innovation and addressing the potential unintended consequences of disruption.

New disruptive financial innovations like Web3 decentralised finance (DeFi), Cryptocurrencies, Blockchain Tokenisation, Play-to-Earn computer games (GameFi) and the Metaverse are prime examples that offer anonymous, borderless, permissionless digital financial ecosystems, but also widen the threat surface for endemic abuse, fraud and cybercrime.

In this presentation, Philip Treleaven, professor of computing at UCL and director of the UK Centre for Financial Computing, reviewed the "tsunami" of disruptive financial innovations; arguing that financial regulation of both traditional and emerging decentralised markets will benefit from a decentralised Big Bang 3.0.

"There's a tsunami of financial innovation hitting us and we have to recognise that most of it is happening in the non-regulated sector," explained Treleaven to delegates. "You've got 16-year-olds giving financial advice to 14-year-olds on TikTok and lots of the innovation is happening in computer games and avatar development."

He also warned delegates about some of the dangers that could crop up as a result of this wave of new technology, including criminals tricking people on the phone by pretending to be a trusted person or company, then recording their voices and using this to access bank accounts via telephone banking for consumers using voice as a method of verification.

"An explosion of financial crime is going to hit us," he warned, adding that regulators need to put forward regulation that is "dynamic and decentralised" to tackle this.

Treleaven spoke about how disparate technologies, from Web 3.0 and DeFi to GameFi and NFTs, have come together to create "the perfect storm".

"Increasingly when interacting with other entities we won't be interacting with a registered company, we'll be interacting with an algorithm," he added.

Now, he said, there are more traditional firms moving towards the same technology used by unregulated ones.

"Where's it going?" he asked, adding that when it comes to Web 3 and DeFi, the industry will see more of a collaborative environment.

"We're moving towards this anonymous world where you don't know what you're dealing with, and these companies will be unregulated," he continued. "Moving towards this digital economy, a lot of innovation is unregulated and risky."

He warned that because a lot of the new innovation is coming from the unregulated sector, increasingly it will be in the criminal sector too.

"Regulators and the police are poorly equipped to deal with this, so they need to think outside the box," he explained. When it comes to traditional regulation, he explained that regulators are collecting more data but only "reviewing around two per cent of it".

While companies are producing lots of data, it's being analysed only retrospectively, with things moving too fast to keep up, he said.

Panel – sponsored by Smarsh

Hybrid risk: meeting regulatory standards in an era of remote working and digital transformation

This panel looked at the regulation challenges that FSIs face as employees continue to work from home.

Hannah Parvin, senior manager, Deloitte Cyber Risk Service Practise, said that there were more data breaches and more risks with working from home. "You can control technology as an organisation, but people are more relaxed at home and won't think twice about having someone in the room on a private call," she said.

Shaun Hurst, principal regulatory advisor at Smarsh, pointed out that the number of communication channels has increased, adding that these are still proving useful despite a move back to the office. He said that it is a challenge to capture all the information from applications like Zoom and MS Teams as part of GDPR rules.

"There's been a shift in the way that people act, it's not just about the tools they are using. When you're sitting at home in your pyjamas and answering your emails, you're going to have a different attitude than when you're sitting in a suit at your office desk," Hurst said.

Sarah-Rose Perry, head of compliance at Octopus Investments, said that despite compliance training, employees are talking informally about clients on recorded media. Clients have the right to request this data under GDPR regulations, she warned.

"Voice notes can be transcribed easily by a compliance monitoring system. But what about the way people use emojis, facepalms and thumbs and how do we translate that into what it actually means?" Perry said.

Samaroha Das, director of IT risk at Metro Bank said that during the pandemic, businesses had been forced to move quickly and ended up using "work arounds" to cope. Technology can be used to process data, while monitoring software can find out if there are any deviations from the guidelines, he explained.

"Technology is not a silver bullet, you have to make it work for you. It is an enabler, but you have to configure it and train people to use it properly," Das said.

Perry agreed. "It's people that decide to do naughty things, not systems. It's really important to get the right culture and that means hiring the right people. People who want to do the right thing. Thankfully I've come across more people who want to do the right thing than the wrong thing," she said.

Fireside Chat

How can the industry collaborate more effectively to digitally optimise controls and meet regulators' expectations of more effective outcomes in fighting financial crime?

With record fines for AML breaches and proposals for mandatory customer compensation for Authorised Push Payment fraud, firms are under greater regulatory and cost pressures when it comes to fighting financial crime.

In addition, regulators are stress testing the effectiveness of firms' systems in priority policy areas such as sanctions screening. This discussion between Paul Munson, UK director of compliance at Shares and Richard Maton, executive director at the International RegTech Association (IRTA), explored how financial services firms are responding by digitally optimising key areas of their control frameworks to enhance decision-making and outcomes across three lines of defence and better process design.

The session also examined how more effective collaboration

frameworks can reduce barriers to adopting new data sets and tools, and enable better system design through data sharing and public/private partnerships.

"What drives me in technology, is using it in the right places," said Paul Munson.

He gave the example of more than 900,000 Suspicious Activity Reports (SARs) being received by the National Crime Agency (NCA) in the latest financial year. Munson said that while this shows that reports are being submitted, it's unclear whether there are outcomes to gauge from this.

"It's important to use technology smartly – to have a holistic view and leverage digital identity in the right way to assess risk," he told delegates.

Richard Maton said that there has been a strong focus by regulators on financial crime, with financial watchdogs testing the effectiveness of controls as well as stress testing on sanctions.

"Regulators are moving into a more data driven approach using data effectively across firms and looking at financial crime data," added Shares' Munson.

Maton said that looking ahead there will be significant investment in data beyond the US, where it has already been a priority.

"One trend we'll see is having information and stress testing on outcomes," he said. "Another driver we're going to see that relates to data use, is fraud."

He explained that the level of investment in protection against fraud will need to go up and more collaboration will be needed.

Munson said that firms can leverage technology and multiple data sources to achieve a holistic view when it comes to fraud.

"Profile the customer, look at how they log on, and use that as an anti-fraud measure," he said. "Use the technology in the KYC process not just at the start but part of an ongoing process."

He continued: "The way to beat financial crime is around data or intelligence sharing that is GDPR compliant. We make the SARs because we have to, but we should be reporting the most serious stuff."

Panel – sponsored by Novatus Advisory

Ready to refit: RegTech's role in preparing FSIs for the EMIR Refit

The European Market Infrastructure Regulation (EMIR) will undergo a significant shakeup in April 2024. This panel looked at how the EMIR Refit will impact reporting and what steps FSIs should take to prepare for the upcoming regulation.

Hannah Meakin, partner at Norton Rose Fulbright LLP said it was important to remember that the EMIR refit stemmed from the G20 commitment to ensure regulators, authorities and central banks had visibility after the financial crisis.

"The policy initiative only really works if you have enough data being reported in the right ways so that it can be aggregated by different regulators around the world so that they can have a global understanding of what's really happening in the marketplace. We're not quite there yet," she said.

John Kernan, chief executive of REGIS-TR, said that there had been some expectations that double sided reporting would be reduced. The review and what the market had ended up with were different to what they were expecting, he said.

He added that one challenge for firms would be potential divergence between the EU version, which will go live in April 2024, and the UK version which the FCA has announced will go live in September.

"It's not a repetition of the existing standards, it's monumental. It's effectively like having to implement a brand new regime and it is far more complex than the EMIR that was implemented in 2014," Kernan said.

Matthew Ranson, partner, regulatory advisory practice and RegTech at Novatus Advisory said that research had found that those firms that had carried out delegated reporting were less concerned about the implementation than firms that did their own reporting, which surprised him.

"When you talk to the regulator, they are very clear that you can delegate the operation of doing a report, but you cannot delegate responsibility.

"I would expect those firms to have less in house expertise and therefore be very concerned by what is coming up. Delegated reporting shouldn't exist, because the costs of providing sufficient oversight are such that you may as well do it yourself," Ranson said.

Carolyn Jackson, partner at Katten UK, said that due to the complexity, the amount of data and additional reporting standards, there are not going to be a lot of firms who will try to do their own reporting.

"They will turn to third party services providers and there will be much more standardisation rather than proprietary methods of reporting. But one of the things that concerns me is: what will the regulators think about it?" she said.

Ranson ended the session by saying that the word "refit" is incredibly unhelpful, as senior executives see it as a "tweak" to existing regulation and may not allocate enough resources to meet the requirements.

Keynote – Prudential Regulation Authority (PRA), The Bank of England

The PRA's work on RegTech and Data in 2023 and beyond

In this closing keynote session, Lewis Webber, head of RegTech, data and innovation at the PRA, talked about the regulator's ambitious work programme to strengthen and transform its data-related capabilities, and how the organisation is collaborating with industry.

Webber began the session by explaining that pre-2021, the PRA took a wide-ranging look at how the financial system could change over a decade. There were many actions involved with this, including leading a RegTech and data strategy within the bank so that it could meet its objectives, he explained.

The head of RegTech talked about how over the past 18 months the regulator has pinned down the strategy more precisely following a review, adding that the organisation has learned lessons from the eight years since it was launched.

"The headline ambition is to deliver a step change in the PRA's efficiency, effectiveness and data culture by 2026," he told delegates, adding that the PRA has organised work into three buckets: how it uses data; how it collects data; and which data it collects.

Webber explained that the guiding principle behind its focus on which kind of data it collects is that the organisation needs to make sure that firms are focussing on the information needed for the PRA to effectively carry out supervision and "possible policy making".

"We need to make sure we are making the best use of the wave of information, which ranges from conceptually straightforward to operationality difficult, and putting it into more sophisticated visualisation tools," he said, adding that the main prize will be an integrated strategy in three years' time.

By the end of this we'll meet all of our goals by creating a single view, customisable supervisory dashboard, that will be best able to probe issues, risks, and policy questions, he said.

"The backbone of info we need is well designed, timely, good quality regulatory reporting received confidentially," he said. "But it's important to say this doesn't always mean more regulatory reporting is better – we need to be proportionate."

He explained that in general, there is currently a gap between reporting and what the PRA needs for day-to-day supervision, adding that it is vital that regulatory reporting is timely and accurate. Webber also talked about some of the many benefits of regulatory reporting, including standardisation.

What was clear from Webber's presentation was that thorough, horizontal reporting needs to look across the entire reporting estate, while at the same time stress testing and removing duplication. Meanwhile, it is necessary to ensure metadata is consistent with common definitions, making end-to-end processes more streamlined and better aligning the data the PRA collects with how it is used.

Webber concluded the event by saying that beyond 2026, when the strategy is completed, it will be highly impactful for the PRA, leading to improvements in how the organisation interacts with firms day-to-day.

FStech Conferences

RegTech Live

SAVE THE DATE

27 FEBRUARY 2024

Follow the event on Twitter: @FStechnology #RegTechLive