FRIL – Innovation to address financial crime

Industry led challenge statements shaping the financial crime programme

FinTech Scotland · University of Glasgow · University of Strathclyde Glasgow · SUPERTECH · Aston University Birmingham UK · Birmingham City University · GMCA Greater Manchester Combined Authority · Greater Manchester Digital Security Hub

Use Case 1

Enhancing security and efficiency in identity verification

TSB · Equifax · Lloyds Banking Group · Money

Use Case 2

Harnessing data to detect evolving typologies of financial crime and fraud

Fujitsu · Equifax · Morgan Stanley · BT · HSBC · abrdn

Use Case 3

Facilitating the proactive and secure sharing of intelligence

NatWest · BT · Money · TSB

Use Case 4

Future proofing systems and controls

Barclays · Lloyds Banking Group · HSBC · Money · Fujitsu

Use Case 5

Strengthening operational efficiencies in alert dispositioning

Morgan Stanley · abrdn · SecureTrust Bank · Barclays · NatWest

FinTech Scotland

Innovation Challenge – Use Case 1

Enhancing security and efficiency in identity verification

Challenge statement: How might we build robust, user-friendly authentication systems to enhance identity verification processes and mitigate risks of emerging threats?

Background: The complexity of identity verification spans both Know Your Customer (KYC) and Know Your Business (KYB) processes. Challenges include accurately identifying and verifying beneficial owners in complex ownership structures, detecting fraudulent or coerced identity documentation, and managing increasingly sophisticated threats such as deepfakes.

Financial institutions are faced with the growing need to balance approval speeds with effectively identifying and mitigating the risks posed throughout the onboarding and ongoing due diligence process.

We are interested in: Advanced, user-friendly authentication systems which enhance security but also maintain a seamless user experience, whilst adapting to evolving threats. Solutions can be applicable to either or both retail and corporate identity authentication scenarios.

Innovation Challenge – Use Case 2

Harnessing data to detect evolving typologies of financial crime and fraud

Challenge statement: How can technology be employed to proactively identify and address evolving financial crime and fraud typologies, leveraging data analytics to enhance risk management capabilities?

Background: The complex spectrum of financial crime and fraud typologies pose an extremely challenging landscape for financial institutions when identifying and disrupting this behaviour. However typically, new typologies do not emerge in a vacuum – there are drivers which may open up new opportunities or drive behaviour in a certain direction for bad actors.

By leveraging internal and external data, as well as insights into socio and geo-political trends, there is an opportunity to proactively detect and address emerging threats, enabling organisations to enhance their risk management capabilities.

We are interested in: Solutions which leverage technology to strengthen the real-time detection, analysis and predictive capabilities of indicators and patterns of evolving threats.

Innovation Challenge – Use Case 3

Facilitating the proactive and secure sharing of intelligence

Challenge statement: How can data related to evolving or confirmed instances of economic crime (including fraud) be shared amongst stakeholders in the ecosystem?

Background: The fight against economic crime is one widely recognised as one which is fragmented, with organisations often privy to only one piece of a much larger jigsaw puzzle. This fragmented nature allows criminals to repeatedly exploit gaps in the system and continue to commit harm.

By leveraging innovative techniques to share data from across the ecosystem in a secure and effective way, whilst ensuring adherence to privacy regulations, there is opportunity to disrupt this activity and proactively prevent harm.

We are interested in: Solutions which facilitate proactive intelligence sharing, real time data exchange and adhere to privacy regulations.

Innovation Challenge – Use Case 4

Future proofing systems and controls

Challenge statement: How can we harness cutting-edge technology to anticipate and address evolving regulatory demands in a proactive, future-focused way?

Background: Financial institutions are navigating an increasingly complex landscape where regulatory requirements and criminal tactics shift rapidly. This demands forward-looking solutions that strengthen the agility in a firm's systems and controls to respond to and go beyond today's standards, ensuring systems are not only compliant but also resilient against future threats.

To stay ahead, financial institutions need to leverage technologies that proactively enhance security, adapt to potential regulatory changes, and strengthen privacy measures.

We are interested in: innovative solutions that anticipate tomorrow's security needs, align with expected regulatory shifts, and future-proof financial systems. The goal is to proactively combat emerging financial threats and facilitate agile and seamless compliance in a dynamic regulatory environment.

Innovation Challenge – Use Case 5

Strengthening operational efficiencies in alert reviews

Challenge statement: How can the applications of technologies, such as generative AI, be leveraged to support the manual review of alerts throughout the KYC process?

Background: Reviewing alerts throughout the KYC process across transaction monitoring, sanctions, PEPs and adverse media, can be manual, time intensive and inefficient. The high volume of alerts, combined with the need to identify and leverage diverse data feeds to make a reasoned risk conclusion places a significant operational burden on teams.

The manual nature of alert reviews in combination with a volume of false positives opens an opportunity for the application of innovative solutions to be applied to stages throughout the KYC process.

We are interested in: exploring solutions that leverage data sources beyond the alert data itself, across both internal and external data feeds. We would like to see solutions that aim to enable a more effective and informed client risk review, for example, utilizing KYC data and to produce an initial level of investigatory commentary and/or prioritisation logic to the alert.