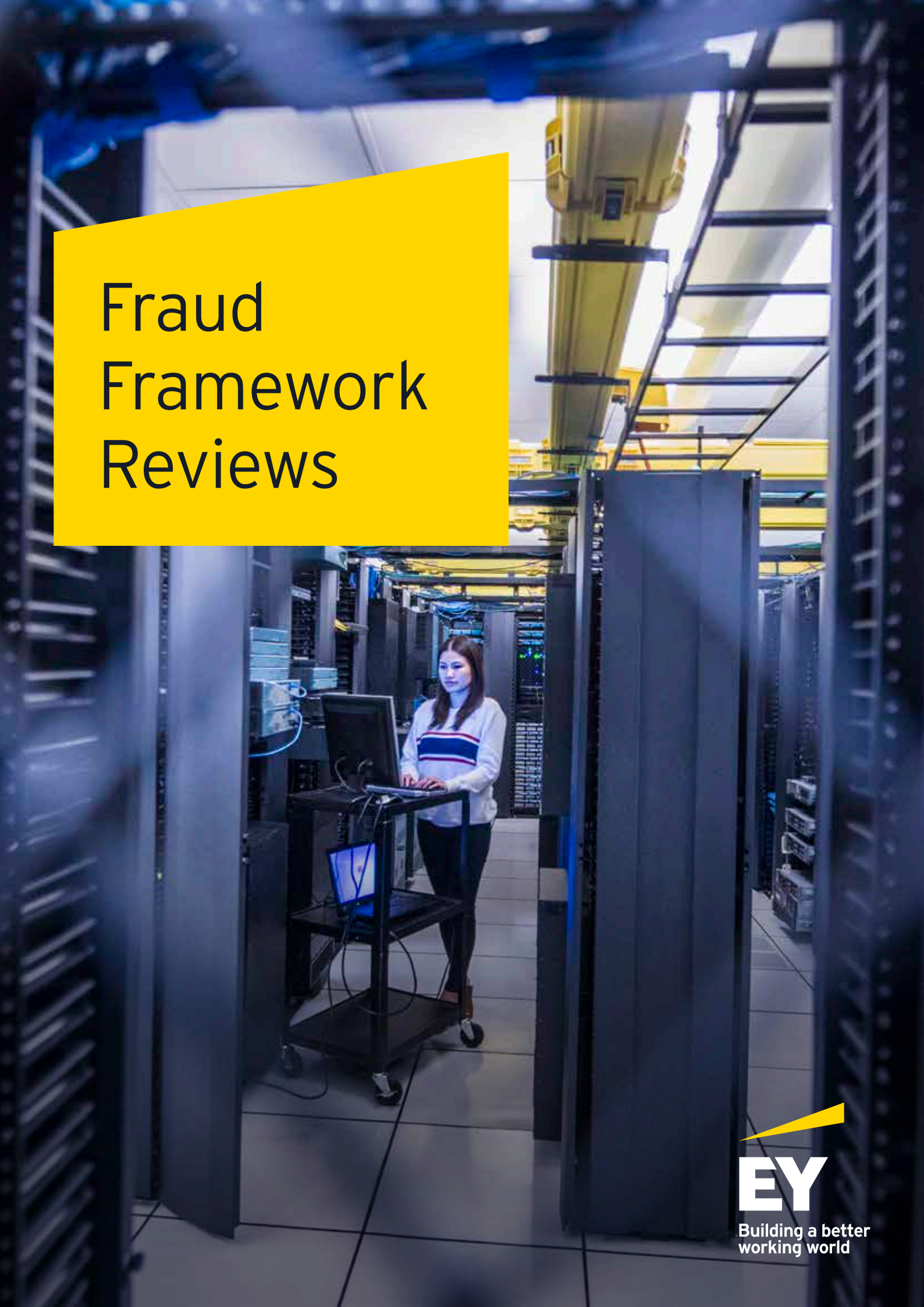
Fraud Framework Reviews



Building a better working world

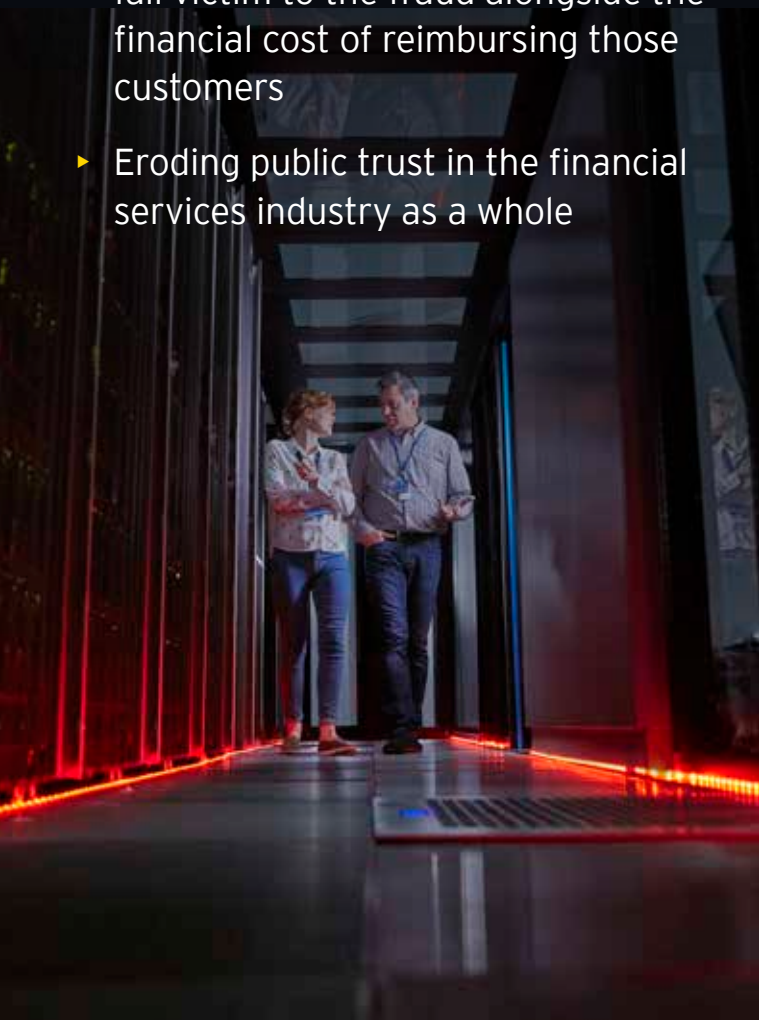
Introduction

UK fraud losses remain at record high levels[1]

Fraud losses in H1 2022	
Unauthorized fraud losses	£360.8m
Authorized push payment (APP) fraud losses	£249.1m

Both unauthorized fraud and APP fraud against UK consumers continue to have significant and varied impacts including:

- The financial and emotional impact on victims
- Reputational damage to financial institutions (FIs) whose customers fall victim to the fraud alongside the financial cost of reimbursing those customers
- Eroding public trust in the financial services industry as a whole



Given the fraud rates in the UK it is unsurprising that there is increased attention from the authorities on how firms are protecting their customers.

Regulatory and government focus

- Given the fraud rates in the UK, it is unsurprising that there is increased attention from the authorities on how firms are protecting their customers:
  - The Financial Conduct Authority (FCA) is increasingly active in the fight against fraud and in its Business Plan 2022/23 announced a number of actions related to reducing and preventing fraud.[2] These include developing its approach to supervising firms' anti-fraud systems and controls, and undertaking a multi-firm review of anti-fraud systems and controls during the year to understand and evaluate how they are protecting consumers from fraud.
  - The Payment Systems Regulator (PSR) has published two consultation papers in the last 12 months covering three main themes:[3] fraud reporting, intelligence sharing and reimbursements with the goal of improvement in fraud prevention controls across the industry. In the most recent consultation paper, it proposes making it mandatory to reimburse victims of APP fraud unless the customer is complicit in the fraud or has been grossly negligent.[4] This shift in liability will dramatically increase the cost of reimbursements for payment service providers (PSPs), and will put more emphasis on ensuring that their anti-fraud controls are effective at mitigating fraud and reducing losses. The proposed 50-50 split of liability for reimbursements between sending and receiving PSP also puts increased emphasis on firms to tighten their controls to detect and prevent money mules, which are currently a key enabler for facilitating fraud.
  - The House of Lords Fraud Act 2006 and Digital Fraud Committee published the findings from their enquiry in November 2022.[5] This includes several key recommendations for how the UK can better tackle fraud going forward, including recommending introducing a "failure to prevent fraud" criminal offense.
  - The Online Safety Bill includes provisions to protect consumers by requiring social media sites and search engines to tackle fraudsters on their platforms.[6]
- Given all of this, it is especially important that FIs ensure that their anti-fraud frameworks are robust and effective at proactively protecting their customers from the harms of fraud in order to stand up to regulatory scrutiny.

---

1 "Half Year Fraud Report 2022", *UK Finance*, ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2022

2 "Business Plans 2022/23", *FCA website*, fca.org.uk/publications/business-plans/2022-23

3 "Publications", *PSR website*, psr.org.uk/publications/consultations/

4 "APP scams, Requiring reimbursement", *PSR website*, psr.org.uk/publications/consultations/cp22-4-app-scams-requiring-reimbursement/

5 "Fraud Act 2006 and Digital Fraud Committee", *UK Parliament*, committees.parliament.uk/committee/582/fraud-act-2006-and-digital-fraud-committee/

6 "Online Safety Bill", *UK Parliament*, bills.parliament.uk/bills/3137

What makes an effective anti-fraud framework?

A robust anti-fraud framework allows FIs to detect and prevent more fraud and to respond sooner to emerging threats. This paper sets out some of the key areas that FIs should focus on when assessing their anti-fraud framework. This isn't an exhaustive list but highlights the main areas. While FIs may have many of these processes and controls in place already, given the rapidly evolving nature of fraud, it is vital to review and assess if they are fit for purpose.

1 Governance and oversight

FIs need to be able to demonstrate that there is appropriate governance in place, showing senior management oversight of and accountability for fraud. This should include the relevant committees and reporting routes to escalate fraud-related issues to the board, and regular escalation of fraud management information (MI) – which should be appropriate for the size and nature of the organization's business and the fraud risks to which it is exposed. FIs should also be able to demonstrate independent oversight of fraud controls from audit or risk oversight teams.

Key questions to ask yourself:

- Is it clear who the owners of fraud risk within the organization are and their responsibilities (aligned to the Senior Managers and Certification Regime, SM&CR[7])?
- Is your fraud MI appropriate for senior management and regulators to understand the fraud risks to which the organization and its customers are exposed?
- When did your last internal audit cover fraud control and governances? Are there any unresolved management action plans since the last internal audit?
- Are the measures you are taking to protect customers from fraud adequate and how do they align to obligations under the Consumer Duty?[8] Do you perform continuous threat assessment and identification of future fraud vectors?

2 Risk-based approach

FIs should be able to demonstrate that they fully understand the fraud risks to which it and its customers are exposed. This can be achieved through maintaining up-to-date fraud risk assessments and detailed fraud risk registers. Fraud risk appetite statements can be used to set the levels of fraud with which the organization is comfortable, and can be used to measure its performance and focus resources.

Key questions to ask yourself:

- How frequently are fraud appetites set? Are they set by fraud typology? How many challenges are they subject to?
- Does the organization fully understand the fraud risks to which it and its customers are exposed?
- When was the last fraud risk assessment conducted and which horizon risks are increasing?
- Do you appropriately quantify the scale of fraud risk you need to mitigate for?

3 People

Fraud teams should be appropriately staffed by individuals with relevant knowledge and experience. This knowledge needs to be kept current with training and education appropriate to the individual's role. Roles and responsibilities of staff involved in anti-fraud activities across the three lines of defense should be clearly defined and documented.

Key questions to ask yourself:

- Are fraud roles clearly defined and documented in an up-to-date Responsible, Accountable, Consulted and Informed (RACI) matrix across the three lines of defense?
- Is there specific training provided to fraud operations and investigations team whose role involves having sensitive discussions with fraud victims?
- How does your second-line fraud team ensure its knowledge is up-to-date?
- Do you have general training and awareness program to highlight latest trends in fraud scams to your customer-facing employees?

7 "Senior Managers Certification Regime", *FCA website*, fca.org.uk/firms/senior-managers-certification-regime
8 "Consumer Duty", *FCA website*, fca.org.uk/firms/consumer-duty

4 Policies and procedures

FIs should have clearly defined fraud policies, explaining how they protect themselves and their customers from fraud. These policies and procedures should be reviewed on a regular basis and refreshed when required. Second- and third-lines of defense should test these to ensure they are embedded, effective and understood by staff.

Key questions to ask yourself:

- Do your fraud policies cover how you protect your customers from fraud, or are they focused on fraud against your organization?
- Are you meeting your obligations under the payment services regulations relating to refunds and reporting?
- Do you have sufficiently detailed procedures for handling APP scam frauds and how do you determine liability?

5 Fraud detection and prevention systems

Having sophisticated anti-fraud systems is key to detecting and preventing fraud; however, the management and governance around these systems are equally important. FIs should ensure that system rules and profiles can be updated in a timely manner to respond to emerging threats. Strong feedback loops and communication between fraud operation teams and fraud data teams are key to quickly identifying trends, increasing the effectiveness of fraud systems, and reducing false positive rates. Where machine learning models are used in fraud systems, appropriate quality assurance (QA) should be performed to ensure the models are learning from accurate data.

Key questions to ask yourself:

- How do you ensure efficient two-way information sharing between fraud operations teams and fraud data analytics teams?
- When was the last independent review over your fraud models or the machine learning model used in your fraud systems?
- Do you have established KPIs and metrics to measure effectiveness of the systems, and what steps do you take in case performance drops?
- Do you have robust fraud detection and prevention technologies in place (e.g., real-time fraud and transaction monitoring, behavioral biometrics, device profiling, geolocation and case management systems)?
- Is there a roadmap or a fraud program in place to revamp existing fraud systems to better address emerging fraud threats?
- How well do you understand the root cause of missed frauds and what corrective action is taken?

6 Data, intelligence and industry engagement

The use of data is increasingly important to detect and prevent fraud. FIs should be able to demonstrate how they are effectively harnessing and using the data available to them, as well as using appropriate external data sources in its fraud systems (e.g., industry fraud databases and consortium data from vendors).

Collaboration within financial services and cross-industry is imperative to quickly respond to threats and facilitate an ecosystem-wide defense against fraud. FIs should consider how they are engaging with their peers and industry bodies to maximize the way in which they share experiences and discuss effective strategies for reducing fraud. Firms may want to consider sharing information related to potential vulnerable victims of fraud, mule accounts and emerging fraud typology information.

Key questions to ask yourself:

- Do you utilize data from the UK-specific fraud databases in your fraud systems?
- Do you play an active role in sharing and utilizing fraud intel from other firms in your fraud framework?
- Is there valuable data and intel in other parts of your business, e.g., financial crime or cybersecurity, which could enhance the effectiveness of current fraud controls? Could these business areas collaborate better to fight fraud and financial crime more effectively?

7 Customer education and awareness

With customers increasingly being targeted by APP fraud, it is important that they are educated and well equipped to identify attempted fraud. FIs should have a clear strategy in place for educating customer-facing staff, raising customers' awareness of fraud and providing tailored warnings to customers when heightened fraud risks are identified.

Key questions to ask yourself:

- Do you have a clearly defined and documented strategy for customer education?
- Are tailored fraud warning messages regularly refreshed and updated to reflect emerging fraud typologies and changes in fraudsters' modus operandi?Do you participate or support industry initiatives aimed at improved customer education and awareness, such as take five and stopscams?

Money mules

While money mules are inherently a money-laundering issue, their use in facilitating and enabling fraud against consumers can't be underplayed. Detecting and preventing money mule accounts by sending and receiving banks is a key way of disrupting and preventing criminals from perpetrating fraud as it reduces their ability to launder the funds. The proposed 50-50 split of reimbursements of APP fraud losses puts increased emphasis on the receiving firms' strengthening of their controls for detecting and preventing money mules. FIs will have to ensure they have robust controls to detect and prevent criminals trying to use its accounts to receive and launder fraudulent funds. This includes enhancing AML controls at onboarding including being able to detect where criminals are using stolen or synthetic identification documents to open accounts. FIs will also have to ensure there is appropriate ongoing monitoring to identify where legitimate customer accounts are subsequently used as mule accounts, for example by using customer profiling to identify uncharacteristic transactions. Fraud systems should have scenarios in place to detect different types of mules including witting and unwitting mule accounts. There is a large overlap between the controls that are used to detect fraud and those which can detect money mule activity, for example the use of customer behavioral profiling. Organizations should therefore ensure their fraud teams and financial crime teams are working together to develop and tune rules and profiles to detect mule account activity.

Next steps

- Given increased scrutiny, now is a good time for FIs to understand the maturity of their anti-fraud framework. We recommend that FIs start by performing a detailed review of their anti-fraud framework to understand the maturity of their controls and identify any areas requiring a refresh or enhancement. This could be followed by reperforming the fraud risk assessment if this hasn't been performed recently.
- FIs should also consider the impact that mandatory reimbursement of APP fraud and greater fraud reporting will have on their fraud strategy and allocation of resources. The increased cost of reimbursements needs to be balanced against investment in tools and enhancements of anti-fraud frameworks, both of which may impact customer journeys.
- FIs should develop a plan identifying the potential impacts of the PSR's APP scam proposals and work with stakeholders across the organization to mobilize the capability enhancements required.
- EY teams can support FIs with conducting a Fraud Health Check service to provide an initial diagnostic, to identify critical gaps in their framework that require urgent attention and identify next steps. Contact us for more details of how we can support you with this.

Key contacts

For further information, please contact the Financial Crime and Forensics team.

Tom Wallbank
Senior Manager, Financial Crime & Forensics, Ernst & Young LLP
T: + 44 20 7951 7410
E: twallbank@uk.ey.com

Ted Rugman
Director, Financial Crime & Forensics, Ernst & Young LLP
T: + 44 20 7951 4331
E: trugman@uk.ey.com

Tom Salmond
Partner, Financial Crime & Forensics, Ernst & Young LLP
T: : + 44 20 7951 8537
E: tsalmond@uk.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG No. 002202-23Gbl
ED None

UKC-027707.indd (UK) 03/23.
Artwork by Creative UK.

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com