FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN
GLOBAL FINANCE & TECHNOLOGY NETWORK

Novel approaches to combat Money Laundering, Terrorism Financing, Fraud, and Scams

February 2025

Executive Summary

Financial crimes, including money laundering, terrorism financing, fraud, and scams, have escalated in both complexity and scale, posing significant threats to global financial stability, integrity, and trust. Despite substantial investments in compliance and regulatory efforts, these illicit activities continue to proliferate, exploiting advancements in technology and the increasing interconnectedness of financial systems.

A recent roundtable organised by the Bank for International Settlements Innovation Hub (BISIH) at the Insights Forum™, held alongside the Singapore FinTech Festival 2024, sought to explore innovative strategies to counter these threats. The roundtable convened experts from financial institutions, payment networks, regulatory bodies, technology firms, academia, and international organisations. Key insights from the discussion highlight the necessity for a holistic and collaborative approach, leveraging advanced technologies, data sharing, behavioural science and regulatory support.

The main takeaways and actionable outcomes from the roundtable include:

1. **Embracing an Ecosystem Perspective**:

   Addressing financial crimes requires a comprehensive strategy that considers all facets of the financial ecosystem and beyond, including financial institutions, fintech players, technology and social media companies, telecommunication providers (telcos), and regulatory bodies.

2. **Leveraging Advanced Technologies**:

   Implementing artificial intelligence, machine learning, and privacy-enhancing technologies can significantly enhance the detection and prevention of financial crimes.

3. **Enhancing Data Sharing and Collaboration**:

   Overcoming legal, technical, and competitive barriers to data sharing is crucial for effective collaboration and collective defence against financial crimes.

4. **Integrating Behavioural Science**:

   Understanding human behaviour is essential in designing interventions that effectively prevent individuals and businesses from falling victim to scams and fraud.

5. **Regulatory Support and Innovation**:

   Regulators play a pivotal role in fostering innovation, providing flexible frameworks, and encouraging the adoption of new technologies while ensuring financial system integrity.

6. **Future Directions and Recommendations**:

   Actionable steps include strengthening public-private partnerships, investing in research and development, prioritising consumer education, and promoting ongoing dialogue and international cooperation.

1. The Escalating Complexity of Financial Crimes

Financial crimes such as money laundering, terrorism financing, fraud, and scams have long plagued the global financial system, undermining financial integrity and eroding public trust. In recent years, the scale and sophistication of these crimes have intensified. Estimates from 2023 indicate that approximately **$3.1 trillion** was laundered globally, while global fraud losses reached an estimated **$485 billion**. Money laundering activities accounted for approximately **2-5% of global GDP**, highlighting the pervasive nature of the problem. Despite financial institutions having invested an estimated **$274 billion** in compliance efforts, there has not been a corresponding decrease in financial crimes. This points to the lack of effectiveness of current approaches and the urgent need for innovative strategies.

The convergence of rapid technological advancements and the globalisation of financial services has transformed the landscape of financial crimes. Criminal organisations have adeptly harnessed crypto-currencies, artificial intelligence (AI), machine learning, and dark web platforms to obstruct conventional surveillance, with illicit transactions increasing from USD 7.8 billion in 2020 to USD 14 billion in 2021. They operate sophisticated networks that transcend national borders, making detection and enforcement increasingly challenging for individual institutions and jurisdictions.

Efforts to combat these threats are hindered by fragmented data and inconsistent regulations. Financial information typically exists in isolated silos, limiting comprehensive analysis. Divergent data protection laws complicate the sharing of sensitive data, even when it is critical for detecting potential crimes. Meanwhile, the convergence of cybercrime, fraud, money laundering, and terrorist financing highlights the interconnected nature of illicit activities.

2. The Imperative for a Holistic and Collaborative Approach

Combatting financial crimes effectively requires a comprehensive view of the entire financial ecosystem and beyond. Roundtable participants emphasised that dismantling silos, so that compliance, cybersecurity, fraud prevention, and AML/CFT units can collaborate directly is essential. Close coordination with technology companies, telcos, and social media platforms could help address fraud and scams that often begin outside the financial ecosystem (e.g. via social media) and ultimately conclude as fraudulent transactions in the financial ecosystem.

Public-private partnerships prove indispensable, facilitating the flow of intelligence, best practices, and resources. High-level government commitment provides policy leadership, resources, and legislative support. Secure information-sharing mechanisms, whether dedicated platforms or networks, help participants

communicate swiftly. Joint task forces among law enforcement agencies, regulators, and industry enhance overall effectiveness. Harmonising regulations, strengthening Mutual Legal Assistance Treaties, and adhering to global standards such as those issued by the Financial Action Task Force (FATF) further reduce cross-border inconsistencies. Actionable steps involve creating formal frameworks for collaboration, implementing secure real-time communication channels, and fostering a culture of shared responsibility in the fight against financial crimes.

3. Leveraging Advanced Technologies and Data Analytics

Advanced technologies are essential for detecting and preventing financial crimes. AI and machine learning models can analyse large datasets to identify anomalies that conventional rule-based models might miss; behavioural analytics can detect deviations from standard customer patterns, revealing signs of potential fraud. Privacy-enhancing technologies (PETs) such as federated learning or homomorphic encryption allow entities to collaborate without compromising sensitive data.

Challenges remain: effective AI systems need consistent, high-quality data, yet information is frequently fragmented, and divergent data protection regulations impose strict datahandling requirements. Complex AI models can also lack transparency, necessitating explainability to build stakeholder and regulatory trust. To address these issues, participants highlighted the importance of robust data infrastructures, adopting PETs for secure collaboration, working closely with regulators to ensure compliance, and forming cooperative data-sharing agreements among institutions.

4. Enhancing Data Sharing and Overcoming Barriers

Data sharing is vital but compounded by legal, competitive, and technical challenges. Divergent data-protection laws may complicate cooperative efforts, even when such cooperation is pivotal to deter criminal activities. Varying data standards also complicate interoperability. Proposed solutions include legal frameworks enabling responsible data sharing with adequate safeguards, along with standardised taxonomies & identifiers to streamline interoperability.

Case studies illustrate success through Information Sharing and Analysis Centers (ISACs), where sector-wide threat intelligence strengthens collective defences, and National Scam Response Centers enhance coordination between financial institutions and law enforcement agencies to rapidly tackle reported scams. To move forward, institutions must engage with legislators and regulators to refine the legal environment, adopt common industry data standards, and invest in secure platforms that protect data while facilitating collaboration.

5. Integrating Behavioural Science into Prevention Strategies

Human vulnerabilities lie at the heart of many financial crimes. Behavioural science insights can help thwart perpetrators' techniques whether by tactically inserting cognitive pauses or warnings into high-risk transactions or crafting culturally tailored messages to better convey the severity of risks. Educational campaigns employing cognitive and behavioural approaches can further protect the public from falling victim to evolving scams. However, individuals under stress or urgency may not respond to rational warnings, and different demographic segments may require tailored interventions.

Organisations like banks and fintechs are already experimenting with interactive interventions such as dynamically adjusting prompts based on user responses and establishing internal behavioural insights teams. Future steps include bringing in behavioural experts during prevention strategy design, developing adaptive systems that respond to real-time cues, and engaging social media and telcos to help neutralise social engineering tactics.

6. Regulatory Support and Innovation

Regulators are pivotal in fostering innovation, while promoting safety and integrity of the financial system. Principles and outcome-based regulation may spur innovation among institutions in meeting compliance requirements, while regulatory sandboxes allow controlled experimentation with innovative solutions. Ongoing dialogue between regulators and industry is essential, ensuring proactive adaptation to emerging technologies. Regulatory harmonisation reduces opportunities for criminals to exploit regulatory arbitrage caused by fragmented legal frameworks.

Keeping pace with technology and balancing innovation against risk are vital. Proactive measures include issuing clear guidance around AI and PETs, encouraging

innovation through accelerators and similar initiatives, enhancing regulatory and supervisory technology (RegTech and SupTech) for improved oversight, and creating secure channels for sharing critical information between regulators and financial institutions.

Conclusion and next steps

The roundtable underscored the urgent need for a comprehensive and collaborative approach to combat financial crimes in an increasingly digital and interconnected world. Participants agreed that while technology plays a critical role, it must be complemented by supportive regulatory frameworks, cross-sector collaboration, integration of behavioural science, and a strong emphasis on collaborative data sharing and privacy protection.

Key Takeaways

- **Data is fundamental**: Access to high-quality data is crucial. Overcoming barriers to data sharing requires collaboration, innovation, & supportive legal frameworks.
- **Technology as a tool**: Advanced technologies like AI and machine learning are essential but must be integrated thoughtfully, with attention to privacy and ethical considerations.
- **Behavioural science integration**:
  Understanding human behaviour enhances the effectiveness of prevention strategies and interventions.
- **Regulatory support is crucial**:
  Regulators must balance enabling innovation with ensuring the safety and integrity of the financial system.
- **Collaboration is essential**:
  Unified efforts across sectors and borders are necessary to address transnational financial crimes effectively.
- **Consumer protection**:
  Protecting consumers and maintaining trust in the financial system are fundamental goals that underpin all efforts.

Participants expressed optimism that through collective efforts and coordination, significant progress can be made in combating financial crimes. The insights and recommendations from the roundtable are intended to inform future initiatives and encourage broader participation from all stakeholders to address these critical challenges.

Note: This report has been prepared in accordance with the Chatham House Rule. Specific identities and affiliations of participants have been omitted to allow for open and candid dialogue while respecting confidentiality. The insights and recommendations are based on a synthesis of expert discussions.

References

Chainalysis Team (2022). Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity. [online] Chainalysis. Available at: https://www.chainalysis.com/blog/2022-crypto-crime-reportintroduction [Accessed 2 Jan. 2025].

Monetary Authority of Singapore (2017). FS-ISAC and MAS to strengthen cyber information sharing across nine countries. [online] Available at: https://www.mas.gov.sg/news/mediareleases/2017/fs-isac-and-mas-to-strengthen-cyber-information-sharing-across-ninecountries [Accessed 2 Jan. 2025].

Nasdaq and Verafin (2024). 2024 Global Financial Crime Report. [online] Available at: https://nd.nasdaq.com/rs/303-QKM-463/images/2024-Global-Financial-Crime-ReportNasdaq-Verafin-20240115.pdf [Accessed 2 Jan. 2025].

Global Finance &
Technology Network (GFTN)

89 Neil Road, #02-04, Singapore 088849
gftn.co | hello@gftn.com