Virtual technical training on

Cyber-Enabled Fraud: Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks

Date: Tuesday, 10 November 2026
Time: 11.00-12.30hrs (Mauritius Time)

Register now

Background

The rapid digitalisation of financial services has created new opportunities for cyber-enabled fraud, including phishing, identity theft, online scams and artificial intelligence-driven deepfakes, exposing individuals and financial institutions to increasingly sophisticated threats.

The proceeds of such crimes may be channelled through financial systems and cross-border transactions, creating significant risks of money laundering, terrorist financing and proliferation financing.

The technical training will explore emerging trends and regional experiences to strengthen the detection, prevention and mitigation of technology-enabled financial crime.

Contacts

☎ 4045652

rce@fscmauritius.org

rcemauritius.org / fscmauritius.org

	Opening Remarks/ Address
11:00-11:05	Mr Nicolas Pinaud, Deputy Director, Directorate for Financial and Enterprise Affairs & Head of Delegation, OECD to FATF
	Keynote Address
11:05-11:10	Mrs Divanandum (Prabha) Chinien, Chief Executive, Financial Services Commission, Mauritius.
Session 1	**Cyber-Enabled Fraud**
11:10-11:30	This session will draw on the FATF's report and analysis, and explore how criminals exploit digital technologies, online platforms and electronic payment systems to commit fraud, move illicit proceeds and conceal the origin or destination of funds. It will highlight key vulnerabilities, emerging threats and relevant measures to strengthen the detection, prevention and mitigation of financial crime risks. **Speaker:** Mr Benjamin Boulay, Policy Analyst (AML/CFT), FATF Secretariat
11:30-11:45	Questions and Answers
Session 2	**Before the First Click: Preemptive Intelligence Against AI-Enabled Financial Crime**
11:45-12:10	The session will explore the evolving AI-enabled fraud landscape, including agentic AI, deepfakes, voice cloning and sophisticated malware, and how emerging threats can be identified through digital footprints, infrastructure patterns and intelligence-led detection. Drawing on an anonymised case study of a major global bank with regional operations, it will demonstrate how a deepfake-enabled impersonation and phishing network was mapped and attributed before launch, highlighting early-warning indicators. **Speaker**: Mr Fin O'Leary, Managing Director, Middle East & Africa (MEA), Blackwired
12:10-12:25	Questions and Answers
	Concluding Remarks
12:25- 12:30	Key takeaways and implications
Coordination by Ms Kheertee Ramsohok, Head of the Regional Centre of Excellence	