SIDC
www.sidc.com.my

ACFE
Association of Certified Fraud Examiners
Malaysia Chapter

SIDC-MACFE FRAUD CONFERENCE 2026

22 April 2026
Securities Commission Malaysia

Combating **Digital Threats** and **Fraud** to **Safeguard Organisational** and **Market Integrity**

ACFE
Association of Certified Fraud Examiners
7.7 Global CPE Points

CPE Eligible

REGISTERED HRD CORP TRAINING PROVIDER
MyCoID:765264K

HRD CORP CLAIMABLE

PROGRAMME OVERVIEW

Fraud is evolving at machine speed, driven by artificial intelligence, instant payments and borderless digital platforms. Criminals now industrialise deception with synthetic identities, deepfakes and automated scam operations, exploiting gaps in governance and controls.

The SIDC–MACFE Fraud Conference 2026 convenes regulators, law enforcement, financial institutions and public-listed companies to address this next wave of digital and online fraud.

Through visionary keynotes, expert panels and case-led discussions, the programme explores the need to fight AI with AI, strengthen KYC/AML and data-privacy practices, as well as coordinate rapid enforcement and remediation.

Participants will gain key take ways from practical tools shared in order to enhance organisational resilience, uphold ethical conduct and protect investors' confidence as well as market integrity across the Malaysia's financial ecosystem.

PROGRAMME OBJECTIVES

- The 2nd SIDC–MACFE Fraud Conference 2026 aims to strengthen the collective response against the accelerating wave of AI-driven and technology-enabled fraud.
- It provides a collaborative platform for capital-market professionals, financial institutions, listed companies, regulators, law-enforcement agencies and technology experts to share insights, analyse real cases and discuss strategies that integrate innovation with governance.
- Through insightful keynotes, interactive panels, forward-thinking dialogues, participants will gain useful tools which could strengthen organisational resilience, protect investor's confidence, uphold ethical conduct as well as market integrity

LEARNING OUTCOMES

By the end of the conference, participants will be able to:

- describe how advances in AI are enabling fraud to become an automated and scalable industry that has impacted organisational governance and resilience
- examine how AI-generated synthetic identities exploit weaknesses in KYC and due-diligence checks
- discuss how deepfakes undermine organisational integrity and public trust
- evaluate how artificial intelligence can be effectively and responsibly deployed to counter AI-driven fraud
- discuss recent enforcement cases and governance lessons important in enhancing integrity and accountability
- discuss how job-scam syndicates use both human trafficking and digital fraud
- analyse early-warning signs and innovative methods to improve organisational resilience and market integrity

AGENDA

8.30 am — Connect at Coffee

9.00 am — Welcome Remarks
Tengku Zarina Tengku Chik Chief Executive Officer, Securities Industry Development Corporation (SIDC)

9.05 am — Opening Remarks
TBC

9.15 am — Keynote Address
TBC

9.30 am — Session 1
Governance and Integrity: How AI Is Reshaping Organisational Defense
As fraud becomes industrialised through automation, synthetic identities, and deepfake impersonation, organisations must strengthen governance, ethics, and leadership oversight to stay ahead. This session connects emerging AI-driven fraud threats with the governance structures, internal controls, and ethical cultures needed to manage them, highlighting how oversight frameworks must evolve in a world where fraudsters use self-learning technologies to bypass traditional defenses.

- **Board and Senior Management Oversight** – How boards and senior management strengthen fraud oversight, accountability, and risk ownership in an AI-driven environment.
- **Integrity and Ethical Leadership** – Why fraud prevention starts with tone from the top, a strong ethics culture, and clear leadership expectations.
- **Stronger Controls for New Risks** – How existing controls (KYC, surveillance, internal audit, whistleblowing) must be updated to handle adaptive malware, synthetic identities, and online scams.
- **AI-Risk Governance and Industry Collaboration** – The need for clear AI-risk policies, ethical use of technology, and closer coordination between regulators, market operators, and industry.

10.25 am — Coffee Break and Networking

10.45 am — Session 2
Synthetic Identity Crisis - When "People" Don't Exist
With generative AI, criminals can now create synthetic identities—digital personas built from real and fabricated data that appear legitimate enough to open accounts, trade, seek financing, and bypass KYC controls. This session explores the rise of synthetic-identity fraud across financial institutions, e-commerce, and regulatory systems, highlighting how AI-generated documents, profiles, and transaction patterns evade traditional safeguards. It also outlines key detection challenges, regulatory expectations, and emerging solutions to protect market integrity from identities that never truly existed.

- **Birth of the Synthetic Identity** – How generative AI fuses stolen and fabricated data to create realistic "persons" with full digital footprints.
- **Financing the Fake** – How synthetic identities are used to open accounts, apply for credit, and move illicit funds through regulated systems.
- **The KYC Blind Spot** – Why traditional onboarding and verification methods fail to detect AI-generated identities in capital-market and fintech ecosystems.
- **Beyond Verification – Building Trust by Design** – How institutions can deploy behavioural analytics, digital-identity frameworks, and regulatory collaboration to combat synthetic-identity fraud.

AGENDA

11.45 am — Session 3

The Deepfake Dilemma - Protecting Brand, People and Truth

As generative AI accelerates, deepfakes have become powerful tools for impersonation, market manipulation, and social-engineering fraud, blurring the line between real and fake. This session examines how deepfakes are created, how they are weaponised in financial and reputational attacks, and the defences organisations can use to authenticate truth and protect trust in an era of AI-generated deception.

- **The Science of Deception** – How generative AI models create convincing voice and video forgeries that evade traditional verification.
- **Impersonation Economy** – Real-world cases of executive deepfakes, social-engineering scams, and market-moving misinformation.
- **Legal and Ethical Minefields** – Regulatory and evidentiary challenges of deepfake use in fraud, defamation, and governance.
- **Defending Truth and Trust** – Cybersecurity, media-forensics, and organisational controls to detect, prevent, and respond to deepfake incidents.
- **The competencies and frameworks** needed to integrate fraud detection into compliance and audit functions

12.35 am — Networking Lunch

2.00 pm — Session 4

Fighting AI with AI - The Next Gen of Fraud Detection

This session explores how AI can be used to detect AI-driven fraud, from fabricated documents and falsified data to manipulated financial evidence. It highlights real examples, key warning signs, and modern verification techniques that help organisations identify digital deception and strengthen trust in financial reporting.

- **AI-Generated Documents and Falsified Data** – How generative AI produces highly realistic falsified documents, records, and datasets that can bypass conventional verification methods.
- **Red Flags and Digital Manipulation Risks** – Key indicators of AI-enabled falsification, including abnormal metadata patterns, inconsistent formatting, and irregular data structures within financial evidence.
- **AI-Driven Alterations to Financial Evidence** – How AI can fabricate ledger entries, manipulate audit trails, or construct synthetic identities that support fraudulent transactions.
- **Strengthening Detection and Governance** – Modern verification tools—such as metadata forensics, anomaly analytics, and authenticity scanners – combined with strong oversight to ensure AI enhances integrity rather than introducing new vulnerabilities.

3.00 pm — Session 5

Enforcement, Collaboration & Rapid Response: Lessons from Real Cases

This session highlights key lessons from recent enforcement actions and showcases how coordinated efforts between regulators, enforcement agencies, and industry players enable faster detection, effective response, and stronger market integrity. It also emphasises the importance of post-incident remediation, control enhancement, and fostering a culture of integrity to restore and maintain stakeholder trust.

- **Insights from Regulatory and Enforcement Actions** – How recent cases reveal gaps in governance, control failures, and compliance weaknesses, offering practical lessons for strengthening oversight and market integrity.
- **Collaboration Models for Early Detection and Response** – How regulators, law enforcement, financial institutions, and market operators work together to identify red flags earlier and coordinate rapid, effective responses to emerging threats.
- **Post-Incident Remediation and Control Enhancement** – Approaches to strengthening systems, processes, and reporting structures following incidents, ensuring lessons learned translate into measurable improvements.
- **Building a Culture of Integrity and Accountability** – How transparent communication, strong leadership, and consistent enforcement actions help rebuild trust and reinforce an ethical, accountable operating environment.

AGENDA

4.00 pm Coffee Break and Networking

4.20 pm Session 6 - Spotlight Session

Trapped by Job Scams and Fraud Networks

This spotlight session uncovers the inner workings of job-scam syndicates that have ensnared thousands across Southeast Asia, revealing how victims are lured with fake employment offers, transported across borders, and coerced into large-scale online fraud operations. Drawing from real cases in Cambodia, Myanmar, and Laos, the session examines the intersection of human trafficking, digital fraud, organised crime, and financial exploitation, shedding light on the growing threat of scam compounds and the implications for organisational awareness and protection.

- **How Job Scams Are Orchestrated** – The recruitment tactics, fake job advertisements, cross-border transit routes, and coercion methods used by syndicates to trap victims.
- **Forced Fraud Operations** – How victims are compelled to run investment scams, romance scams, phishing schemes, and other digital fraud operations under threats and exploitation.
- **The Business Model of Scam Compounds** – The organisational structure, revenue-generation mechanisms, and links to broader global fraud networks that fuel industrial-scale scam operations.
- **Recent Cases and Rescue Operations** – Insights from law-enforcement investigations, real case studies, and regional rescue efforts that reveal how these networks operate and evolve.
- **Organisations' Role in Awareness and Protection** – How companies can strengthen detection mechanisms, protect employees, raise awareness, and support reporting frameworks to mitigate exposure to job-scam networks.

5.25 pm Closing Remarks

TBC

End of programme

JOIN the SIDC-MACFE Fraud Conference 2026

for expert insights, real case studies and collaborative strategies to **safeguard the capital market!**

NORMAL
RM2,000/pax
(before SST)

GROUP OF 5 OR MORE
RM1,620/pax
(before SST)

MACFE MEMBER
RM1,800/pax
(before SST)

Get in touch and speak to our friendly team via mobile / e-mail

Farith Jamal I +6014 653 2578
Farith.Jamal@sidc.com.my

Abdul Qaiyum I +6017-8713242
Qaiyum.Ghazali@sidc.com.my

Sarah Dalina I +6011 2711 9658
Sarah.Dalina@sidc.com.my

Wan Mohd Farid I +6012 641 7589
FaridK@sidc.com.my

Syed Imran I +6017 743 0773
Imran.Nasir@sidc.com.my

SIDC
www.sidc.com.my

Securities Industry Development Corporation (765264K)
3, Persiaran Bukit Kiara, Bukit Kiara, 50490 Kuala Lumpur, Malaysia Email: sidc@sidc.com.my Website: www.sidc.com.my

Find us on Youtube, Linkedin, Facebook & Instagram at Securities Industry Development Corporation - SIDC

** The SIDC reserves the right to amend the programme as deemed appropriate without prior notice.*