Date: 30 April 2026

Notice No: FSRA/FCCP/76/2026

To: Senior Executive Officers (SEO) and Principal Representatives (PR) of FSRA's Authorised Persons & Recognised Bodies

Dear SEO/PR,

Re: Cyber Threats Relevant to Virtual Asset Service Providers

The Financial & Cyber Crime Prevention ("FCCP") Department remains committed to informing FSRA's Authorised Persons & Recognised Bodies (hereinafter referred to as 'Firms') of emerging and inherent cybercrime threats. This notice highlights selected cyber threats of particular relevance to Virtual Asset Service Providers ("VASPs").

Cybercrime activity targeting VASPs is increasing in both sophistication and scale, reflecting the operational and technological characteristics of virtual asset ecosystems. These threats may result in financial loss, data compromise/loss, operational disruption, reputational damage and non-compliance where controls are inadequate.

Firms should ensure their cybercrime prevention frameworks remain effective and proportionate to their business model, size and risk profile and are regularly reviewed to address the evolving threat landscape.

Scope and Objectives

This notice aims to:
1. Highlight a non-exhaustive range of cyber threats relevant to VASPs;
2. Assist Firms in understanding key risk vectors; and
3. Promote the implementation of proportionate, risk-based cyber resilience measures.

This notice does not constitute an exhaustive assessment of all cyber threats affecting the sector.

Overview of Key Cyber Threats

The following cybercrime threats are commonly associated with risks to VASPs:

1. Infrastructure attacks and key compromise

- Theft of Private key / seed phrases: Threat actors may target "hot" wallets (internet-connected wallets), unsecured key storage to steal private keys or seed phrases and execute unauthorised withdrawals.
- Compromise of withdrawal governance: Weak internal controls, insecure development environments or inadequate access management may be exploited to initiate fraudulent transfers.

2. Ransomware and extortion

- Ransomware campaigns: Malware targeting VASPs infrastructure may disrupt critical systems and services and, in some cases seek payment in exchange for decryption.
- Data leakage / double extortion: Attackers may exfiltrate sensitive data prior to encryption and threaten disclosure to increase pressure to pay a ransom.

3. **Deepfake identity fraud and credential theft**
    - AI-generated voice or video impersonation: Threat actors may use synthetic audio or video to impersonate executives, employees or customers to bypass onboarding controls, KYC processes and/or multi-factor authentication (MFA).
    - Credential and key harvesting: Attackers may obtain private keys, passwords or seed phrases through fraudulent websites, social engineering or malicious browser extensions.

4. **Supply chain attacks**
    - Compromise of third-party software and services: Threat actors may target vendors and service providers by introducing malicious code into software updates or open-source dependencies relied upon by VASPs.

5. **Decentralised finance (DeFi) exploits**
    - Cross-chain bridge vulnerabilities: Attackers may target interfaces between blockchains, potentially enabling the unauthorised minting or theft of assets.
    - Flash loan manipulation: Use of large, rapid loans to manipulate token prices and extract value within a single transaction (economic logic exploit).
    - Re-entrancy attacks: Exploitation of smart contract's execution order repeatedly calling a function before the contract state is updated, potentially draining funds in a loop (code flaw exploit).

6. **Emerging threats (horizon scanning)**
    - AI-driven autonomous attacks: Threat actors may use automated tools and AI-enabled techniques to conduct reconnaissance, identify vulnerabilities and execute attacks at scale and speed.
    - Quantum risk to cryptography: Although nascent, advances in quantum computing could eventually compromise widely used cryptographic algorithms and should be considered in longer-term cyber security planning.

Regulatory Expectations and Recommended Actions

Firms are expected to assess their exposure to the risks outlined above and implement proactive, risk-based measures to strengthen cyber resilience. In particular, Firms should consider:

- Implementing strong key custody arrangements, including hardware-backed controls where appropriate and robust withdrawal governance such as multi-signature approval and segregation of duties.
- Ensuring smart contracts and DeFi interactions undergo appropriate security review, testing (including code audits and penetration testing) and continuous monitoring to mitigate exploitable vulnerabilities.
- Embedding security and compliance into system and product design (secure-by-design) including rigorous access management, change controls and secure development practices to reduce the risk of architecture weaknesses.
- Maintaining effective cyber hygiene controls, including timely patching, phishing-resistant Multi Factor Authentication (MFA), continuous monitoring, incident response readiness, third-party risk management and ongoing staff awareness and training, to address the increasing pace and sophistication of AI-enabled threats.

Firms remain subject to the obligation to comply with GEN 3.5 including the requirement to report material IT or cyber incidents to the FSRA within 24 hours of discovery.

Your cooperation and vigilance in implementing effective measures are crucial to maintaining the integrity, security and stability of ADGM and the UAE's financial system.

For any further clarification, Firms are required to reach out by email to fccp-cybercrimeprevention@adgm.com.

Sincerely

Financial & Cyber Crime Prevention