**Date:** 12 December 2025

**Notice No: FSRA/FCCP /179/2025**

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

Dear SEO / PR,

**RE: Announcement of the first FSRA cyber threat intelligence weekly newsletter**

The Financial & Cyber Crime Prevention (FCCP) department are pleased to announce the launch of the first weekly Cyber Threat Intelligence (CTI) newsletter, in alignment with Notice No. FSRA/FCCP/15/2024, which addresses Cyber Security Council Alerts - Indicators of Compromise (IoCs).

The weekly newsletter is an additional resource to support Authorized Persons and Recognized Bodies (collectively referred to as Relevant Persons) in strengthening their overall cyber resilience.

## The Role of CTI in Strengthening Cyber Resilience

The effective dissemination of timely CTI provides several key advantages to FSRA Relevant Persons. It enhances organisational awareness of current and emerging cyber threats. By leveraging timely CTI, organizations can adopt a more proactive stance against cyber threats, by anticipating and preparing for evolving attack methods.

FSRA Relevant Persons are encouraged to establish clear internal accountability for the collection, validation and analysis of CTI and to embed structured processes for distributing relevant intelligence across the organisation. This includes ensuring that CTI reaches functions such as risk management, front-line IT & cybersecurity operations and teams involved in incident response planning.

## Foundational sources of the Newsletter Intelligence

The insights provided in the weekly newsletter is derived from the newly developed FSRA CTI platform. The platform aggregates, analyses and centralises intelligence from a wide range of credible sources and filtered to ensure the intelligence disseminated is not only timely but also actionable and relevant. These sources include, but are not limited to, the following:

1) **The UAE ecosystem** - Strategic threat intelligence from national security agencies including the Cyber Security Council (CSC) and the National Security Operations Centre.
2) **The 'Crystal Ball' -** A multinational cyber threat intelligence platform developed collaboratively by Microsoft and CSC, contributing to the global Counter Ransomware Initiative (CRI)
3) **Global financial ecosystem** - Sector-specific intelligence sourced from financial services organisations worldwide.
4) **Premium commercial feeds** - Threat data obtained from leading subscription based commercial CTI providers.
5) **Open-source Intelligence** - Publicly available threat information from reputable cybersecurity online articles and community groups.

The intelligence shared will be enriched with the latest Threat, Tactics, Procedures (TTP's) and IoC's observed from incidents regionally and globally, enabling organizations to implement defensive measures in a timely manner.

In summary, the weekly newsletter will consist of insights into recent cyber breaches affecting financial institutions, high impact vulnerabilities requiring immediate attention, threat actor campaigns targeting the sector, emerging attack vectors and recommended mitigation strategies.

**Guidelines for reviewing and managing shared threat intelligence**

It is imperative that all intelligence received is handled in line with Traffic Light Protocol (TLP) set by the Cybersecurity and Infrastructure Security Agency (CISA). The TLP is a system used for classifying and handling sensitive information to ensure it is shared with the appropriate audience.

For convenience, the newsletters are organized by intelligence classification (Clear and Amber) to facilitate review and distribution. Relevant Persons (RPs) may share 'Clear' intelligence without restriction. However, 'Amber' intelligence may only be shared with members of RPs own organization on a need-to-know basis.

We encourage all FSRA Relevant Persons to diligently review the intelligence circulated, assess potential exposure and undertake appropriate measures to identify, evaluate and mitigate cyber threats to safeguard their digital infrastructure from crime.

For any further inquiries or clarification, please do not hesitate to contact us at FCCP-cybercrimeprevention@adgm.com

Sincerely,

**Financial & Cyber Crime Prevention**