System Restoration, Investigation Findings, and Compliance Guidance

(August 27, 2025)

Monitoring and validation of systems restoration

We tested our systems over the past weekend by lifting the containment for a period of time on each day and monitored all activity very closely. We tested and confirmed successful access to our systems. No suspicious activity was detected by CIRO or CrowdStrike security teams. All network traffic into and out of our systems was as expected.

For service restoration, priority will be given to systems that Members rely upon for their reporting obligations and access to obtain public information including:

- CIRO Services
- Complaint and Settlement Reporting System (COMSET)
- Continuing Education Reporting and Tracking System (CERTS)
- Mutual Fund Dealers Member-only Site
- EFS
- MTRS Reporting
- Advisor Report
- Corporate and Government Debt Trading Information

A reminder that critical functions including market surveillance have continued to operate effectively throughout this incident, with some workarounds, on infrastructure that was not affected by or contained as part of the investigation and was confirmed as clean and secure.

Compliance with reporting obligations

Firms are expected to meet their regulatory reporting obligations as systems come back online.

- For reporting deadlines that occurred during the outage up to and including Monday, September 1 for those systems that were unavailable, firms will have five (5) business days from the date of notification of system restoration to file those reports.
- For reporting obligations due on or after Tuesday, September 2, firms are expected to submit reports on time and in line with their obligations.

Confirmed findings from our Investigation

As you are aware, CIRO immediately activated our incident response protocols and engaged with technical experts, CrowdStrike. Together, we conducted a thorough investigation, and implemented corrective measures to ensure the integrity, confidentiality, and availability of our systems and services.

We can confirm the following:

- There has been no active threat detected in CIRO’s environment since the systems were contained on August 11.

- The point of entry and scope of the attack were determined and confirmed from the forensic artefacts and investigation, including log files.
- No evidence of malware deployment, including encryption software, was found by CIRO and CrowdStrike's Endpoint Detection and Response (EDR) and forensics software.
- Data in our systems was not manipulated or deleted.

Technical remediation actions taken

We have also taken several technical remediation actions, including:

- All affected systems and services have undergone comprehensive security reviews and technical validation. Machines affected by the incident have been replaced.
- User accounts and software affected by the incident have been deleted.
- Additional security software has been deployed to all machines to protect and proactively respond to known threats.
- The isolation and integrity of our systems backups have been confirmed.
- All login details and access information for CIRO staff and service providers have been reset across the entire environment.
- Dark web monitoring service has been activated and there has been no indication that the information copied has been sold or shared, relating to this incident.