

Cyber & Operational REsilience (CORE)

Cyber threats increasingly target shared infrastructure, including cloud services, authentication platforms, communications tools and other software providers. When one vendor is compromised, dozens or even hundreds of member firms may be affected.

With that in mind, in 2025 FINRA launched CORE to strengthen market resilience by leveraging FINRA's market-wide insight to provide the intelligence needed to identify risks and act before they escalate.

What is FINRA CORE

FINRA CORE is the self-regulatory organization's enhanced cyber and third-party risk intelligence capability, built to identify, assess, and share intelligence on cyber and technology risks impacting member firms and their extended vendor ecosystems. By enhancing visibility across the broker-dealer landscape, CORE enables early detection of vendor-related threats, systemic technology failures and emerging cyber-attack patterns—and delivers actionable insights back to firms.

How it Works

CORE fuses multiple intelligence sources, including:

- member firm responses to FINRA's Third-Party Vendor Request
- open-source intelligence on vendor incidents, vulnerabilities and threat activity
- curated cyber and technology intelligence on firms and their vendors
- dark web monitoring of forums, data dumps and cybercrime chatter
- commercial threat intelligence platforms tracking malicious infrastructure, TTPs and threat actors
- FINRA's internal cyber risk models and supervisory data
- and more

Then upon detecting a breach, vulnerability, emerging risk or other related issue affecting one or more member firms, FINRA delivers actionable intelligence to those impacted firms for immediate response.

This integrated approach enables earlier detection of emerging cyber threats and more proactive regulatory engagement—especially where vendor exposure or systemic risks are involved.

Benefits to FINRA Member Firms

- Deeper visibility into vendor- and technology-related threats
- Timely, targeted intelligence that supports incident prevention and response
- Insight into cross-firm dependencies and ecosystem-wide risk exposure
- Stronger coordination with FINRA on systemic or high-impact cyber events