INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-10 18:37 UTC

# FINRA's Financial Intelligence Fusion Center Signals Regulatory Shift Toward Cyber-Fraud Convergence

GOVERNANCE | MEDIUM | CVSS 5.0

| | |
|---|---|
| SCC Item ID | SCC-GOV-2026-0014 |
| Type | Governance |
| Severity | MEDIUM |
| CVSS Base Score | 5.0 |
| Affected Products | Financial sector organizations regulated by FINRA |
| Published | 2026-04-10T11:52:28 |
| Discovery Source | Rss |

## Executive Summary

FINRA has launched a Financial Intelligence Fusion Center designed to merge cybersecurity threat intelligence with fraud detection across regulated financial institutions. The initiative formalizes that cyber intrusions, particularly credential theft and account takeover, are primary enablers of financial fraud, not separate threat categories. For FINRA-regulated firms, the framework suggests an expectation that security and fraud operations should share intelligence and demonstrate coordinated response capability, not operate as isolated functions.

## Technical Analysis

This is a regulatory governance development, not a vulnerability disclosure. No CVE applies. The fusion center model targets the operational overlap between cyber-enabled fraud techniques and traditional financial crime. Relevant MITRE ATT&CK techniques include T1078 (Valid Accounts, credential-based access enabling account takeover), T1566 (Phishing, initial access for fraud campaigns), T1657 (Financial Theft, direct fraud objective), T1539 (Steal Web Session Cookie, session hijacking enabling unauthorized transactions), and T1114 (Email Collection, intelligence gathering supporting BEC). Associated weakness patterns include CWE-306 (Missing Authentication for Critical Function) and CWE-287 (Improper Authentication), both common in account takeover fraud chains. Threat actors including FIN7 and Scattered Spider have historically conducted credential theft and account takeover fraud; the fusion center is designed to detect these vectors earlier. No patch or vendor advisory exists; the action surface is organizational and programmatic.

## Action Checklist

1. Assess integration gaps: conduct a current-state review of your cybersecurity and fraud operations teams to identify whether threat intelligence, alerting, and case data are shared or siloed. Document gaps before FINRA examination posture hardens around this model.
2. Map detection coverage: verify that your SIEM and fraud detection platforms have bidirectional visibility into account takeover indicators - anomalous authentication events (T1078), session cookie theft signals (T1539), and unusual email access patterns (T1114). Confirm alert routing reaches both security and fraud teams.
3. Review authentication controls: audit critical financial transaction workflows for missing or weak authentication (CWE-306, CWE-287). Prioritize MFA enforcement on high-value account actions, wire initiation, and administrative functions.
4. Establish a joint escalation protocol: define a written procedure for how cybersecurity and fraud operations escalate cross-functional incidents. Assign ownership, communication paths, and SLAs. This is the operational artifact an examiner will ask to see.
5. Benchmark against NIST CSF Respond and Recover functions: align your coordinated cyber-fraud response capability to NIST CSF 2.0 Respond (RS.CO, Communications) and NIST SP 800-53 IR-4 (Incident Handling) to build an audit-ready control narrative.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | STANDARD |
| **Escalation Criteria** | Escalate to immediate priority if FINRA examination notice is received, if an active account takeover incident is identified involving a wire-eligible account, or if the organization cannot produce a joint escalation protocol or cross-functional detection evidence within 72 hours of an examiner inquiry. |
| **Recovery Notes** | Because this threat is regulatory and structural rather than a discrete exploit, recovery means demonstrating a sustained operational posture: after closing identified gaps, run a joint tabletop exercise within 60 days using an ATO-to-wire-fraud scenario to validate the new escalation protocol under simulated conditions and capture the exercise record as an audit artifact. Monitor the FINRA fusion center's published advisories and bulletins on an ongoing basis (subscribe via FINRA.org regulatory notices) to ensure your detection coverage evolves with the threat intelligence FINRA expects firms to act on. Conduct a quarterly review of cross-team alert routing to confirm that SIEM rule changes or fraud platform upgrades have not re-siloed visibility into T1078, T1539, and T1114 indicators. |

| | |
|---|---|
| **Forensic Artifacts** | Identity provider authentication logs (Okta system logs, Azure AD Sign-In logs, or Windows Security Event Log Event IDs 4624/4625/4648) filtered for accounts in wire-transfer approval and financial admin groups — these directly evidence T1078 (Valid Accounts) exploitation as the cyber precursor to wire fraud \| Microsoft 365 or Google Workspace Unified Audit Logs for MailItemsAccessed, MessageBind, and FileAccessed operations on accounts with financial transaction authority — evidences T1114 (Email Collection) pre-fraud reconnaissance that the FINRA fusion center model specifically targets \| SIEM alert rule export and notification routing configuration — documents which detection rules for T1078, T1539, and T1114 exist, what their thresholds are, and whether fraud operations are included as alert recipients, establishing the integration gap baseline \| Fraud case management system records cross-referenced against security incident tickets for the prior 12 months — identifies cases where cyber intrusion and fraud activity co-occurred but were handled in separate silos without joint escalation, which is the core evidentiary gap FINRA's fusion center model is designed to close \| MFA enrollment and enforcement reports from the IdP for accounts with wire initiation, wire approval, and financial system administrative privileges — directly evidences CWE-306 (Missing Authentication for Critical Function) and CWE-287 (Improper Authentication) exposure on the highest-value ATO targets |

### Per-Action IR Details

**Assess integration gaps — conduct a current-state review of your cybersecurity and fraud operations teams to identify whether threat intelligence, alerting, and case data are shared or siloed. Document gaps before FINRA examination posture hardens around this model.**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Establishing IR capability, policies, and cross-functional coordination structures before an incident occurs

**Controls:** NIST IR-4 (Incident Handling) — requires an incident handling capability that coordinates across organizational functions, NIST IR-8 (Incident Response Plan) — mandates a documented IR plan that assigns roles, responsibilities, and communication paths, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — requires that audit records be reviewed and shared with relevant parties to support detection and response, CIS 8.2 (Collect Audit Logs) — establish that logging is enabled across enterprise assets and accessible to both security and fraud teams

**Compensating:** Using a shared spreadsheet or ticketing tool (e.g., free-tier Jira, Trello, or a shared Confluence page), build a gap matrix: list each detection signal type (ATO alert, wire fraud flag, credential theft IOC) and map which team currently receives it. Conduct a tabletop walkthrough with both teams using a simulated account takeover scenario to surface handoff failures in real time. Total tooling cost: zero.

**Evidence:** Before formalizing findings, snapshot the current state of alert routing: export SIEM alert rule configurations showing destination notification groups (do fraud operations appear as recipients on T1078/T1539 detection rules?); pull fraud case management system logs showing whether cyber incident ticket numbers are cross-referenced in fraud cases; document whether the fraud platform (e.g., NICE Actimize, SAS Fraud, or internal tooling) has any API or feed integration with the SIEM. These artifacts establish your pre-remediation baseline and will be the examiner's first ask.

**Map detection coverage — verify that your SIEM and fraud detection platforms have bidirectional visibility into account takeover indicators: anomalous authentication events (T1078), session cookie theft signals (T1539), and unusual email access patterns (T1114). Confirm alert routing reaches both security and fraud teams.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring for indicators of compromise, correlating signals from multiple sources, and ensuring alert coverage reaches all relevant responders

**Controls:** NIST SI-4 (System Monitoring) — requires monitoring of information systems to detect attacks and indicators of potential attacks, NIST AU-2 (Event Logging) — requires identification and logging of event types

necessary to support detection of credential abuse and session manipulation, NIST AU-3 (Content of Audit Records) — audit records must capture who, what, when, and where to support ATO and session theft analysis, NIST IR-5 (Incident Monitoring) — requires tracking and documenting incidents, which presupposes that alert pipelines reach all stakeholders, CIS 8.2 (Collect Audit Logs) — ensure logging is enabled across all assets that handle authentication and email access, feeding both SIEM and fraud platforms

**Compensating:** For teams without a commercial SIEM, deploy Sysmon with the SwiftOnSecurity Sysmon config to capture process and network telemetry, then forward logs to a free ELK stack or Graylog CE instance. For T1078 (Valid Accounts abuse): query Windows Security Event Log for Event ID 4624 (Logon Success) and 4625 (Logon Failure) filtered on Type 3 (Network) and Type 10 (RemoteInteractive) for privileged financial application accounts. For T1539 (Steal Web Session Cookie): monitor IIS or Apache access logs for session token reuse from mismatched source IPs or User-Agent strings. For T1114 (Email Collection): query Microsoft 365 Unified Audit Log (via Search-UnifiedAuditLog PowerShell cmdlet) for MailItemsAccessed and MessageBind operations from non-standard clients or unexpected IP ranges. Publish a Sigma rule per technique so manual log review is repeatable.

**Evidence:** Before tuning rules, export the current SIEM detection rule inventory and confirm whether rules exist for MITRE T1078, T1539, and T1114 — note which rules have fraud team notification configured vs. security-only. Pull a 30-day sample of authentication logs from the identity provider (Okta system logs, Azure AD Sign-In logs, or on-prem AD Security Event Log) and flag accounts that authenticated successfully from two geographically distinct IPs within a 1-hour window (impossible travel, a primary ATO precursor). Capture Microsoft 365 Unified Audit Log entries for MailItemsAccessed events occurring outside business hours for accounts with wire initiation privileges — this directly evidences T1114 pre-fraud reconnaissance.

**Review authentication controls — audit critical financial transaction workflows for missing or weak authentication (CWE-306, CWE-287). Prioritize MFA enforcement on high-value account actions, wire initiation, and administrative functions.**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Hardening authentication controls on high-value workflows reduces the attack surface that credential theft (T1078) and session hijacking (T1539) exploit to enable financial fraud

**Controls:** NIST IA-2 (Identification and Authentication — Organizational Users) — requires MFA for privileged and high-impact user actions, directly addressing CWE-306 (Missing Authentication for Critical Function), NIST IA-8 (Identification and Authentication — Non-Organizational Users) — extends authentication requirements to external users accessing financial transaction portals, NIST AC-3 (Access Enforcement) — enforces approved authorizations for logical access to transaction workflows, limiting blast radius of compromised credentials, CIS 6.3 (Require MFA for Externally-Exposed Applications) — mandate MFA on all externally-facing financial portals and transaction initiation interfaces, CIS 6.5 (Require MFA for Administrative Access) — require MFA for all administrative accounts, including those with wire transfer approval authority

**Compensating:** For organizations that cannot deploy enterprise MFA immediately: use free TOTP-based MFA (Google Authenticator or Aegis paired with a TOTP-capable VPN or application layer) for administrative and wire-initiation accounts as an interim control. Run a PowerShell audit against Active Directory to identify all accounts with delegation rights or financial application admin group membership that lack MFA enrollment: Get-ADUser -Filter * -Properties * | Where-Object {$_.MemberOf -match 'WireApprover' -and $_.mfa_enforced -ne $true}. Document all CWE-306 findings (workflows reachable without step-up authentication) as compensating control exceptions with a remediation target date — this documentation is what a FINRA examiner will review.

**Evidence:** Before remediating, capture the authentication configuration state as evidence of the pre-remediation posture: export Identity Provider (IdP) MFA enrollment reports (Okta Admin → Reports → MFA Enrollment, or Azure AD → Authentication Methods → Registration Details) filtered for accounts in wire-transfer and admin security groups. For on-prem environments, run dsquery or PowerShell to enumerate AD group members with financial application access and cross-reference against your MFA enrollment list. Screenshot or export workflow configurations in your core banking or wire initiation system (e.g., FIS, Fiserv, Jack Henry) showing step-up authentication requirements — or the absence thereof. These artifacts document CWE-306 and CWE-287 exposure for both internal risk records and potential regulatory inquiry.

**Establish a joint escalation protocol — define a written procedure for how cybersecurity and fraud operations escalate cross-functional incidents. Assign ownership, communication paths, and SLAs. This is the operational artifact an examiner will ask to see.**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Developing written escalation procedures and cross-functional communication paths is a core preparation requirement; NIST 800-61r3 explicitly identifies the IR plan, communication procedures, and defined roles as foundational artifacts

**Controls:** NIST IR-4 (Incident Handling) — requires a defined incident handling capability covering preparation, detection, containment, eradication, and recovery, with explicit coordination across functions, NIST IR-6 (Incident Reporting) — requires personnel to report suspected incidents through defined channels within specified timeframes, NIST IR-8 (Incident Response Plan) — mandates a documented IR plan that includes roles, responsibilities, and communication paths; this joint escalation protocol is a required artifact of IR-8 compliance, NIST IR-7 (Incident Response Assistance) — requires an IR support resource capable of advising cross-functional stakeholders, which this joint protocol operationalizes, CIS 7.2 (Establish and Maintain a Remediation Process) — a risk-based escalation and remediation process with defined owners and SLAs maps directly to this control

**Compensating:** Draft the joint escalation protocol using a one-page runbook template (available free from CISA's Resources library) that defines: (1) triggering conditions — which ATO signals or fraud alerts require joint escalation (e.g., credential theft IOC matched to an account with a pending wire); (2) primary contacts and backups for both security and fraud teams; (3) SLA tiers (e.g., joint triage within 30 minutes for active wire fraud, 4 hours for post-hoc ATO discovery); (4) communication channel (dedicated Slack channel, Teams channel, or bridge line). Store the runbook in a location both teams can access without authentication barriers during an incident.

**Evidence:** Before drafting the new protocol, preserve evidence of the current escalation posture: collect any existing SOC escalation matrix or fraud alert runbooks and document whether cross-team escalation is covered. Pull the last 90 days of major incident tickets from both the security ticketing system and fraud case management system and identify cases where both teams were involved — note average time-to-cross-team-notification as a baseline SLA metric. This baseline data demonstrates due diligence in gap identification and gives the new SLA targets a defensible foundation for examiner review.

**Benchmark against NIST CSF Respond and Recover functions — align your coordinated cyber-fraud response capability to NIST CSF 2.0 Respond (RS.CO — Communications) and NIST SP 800-53 IR-4 (Incident Handling) to build an audit-ready control narrative.**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, policy updates, and control narrative development align to the post-incident phase, which in NIST 800-61r3's CSF 2.0 mapping corresponds to the Govern and Identify functions as well as retrospective improvement of the Respond capability

**Controls:** NIST IR-4 (Incident Handling) — the foundational control this benchmark exercise validates; the control narrative must demonstrate that preparation, detection, containment, eradication, and recovery capabilities exist and are tested for cyber-fraud convergence scenarios, NIST IR-3 (Incident Response Testing) — requires regular testing of IR capability; the benchmark should identify gaps that trigger a tabletop exercise specifically covering ATO-to-wire-fraud escalation scenarios, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — an audit-ready control narrative for FINRA must demonstrate that audit records from both cyber and fraud systems are reviewed, correlated, and reported, NIST SI-5 (Security Alerts, Advisories, and Directives) — demonstrates that the organization receives and acts on regulatory and threat intelligence inputs (including FINRA fusion center outputs) as part of its control framework, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — a documented, reviewed vulnerability and risk management process is a prerequisite for building a credible audit-ready narrative

**Compensating:** Use the free NIST CSF 2.0 Online Informative References tool (csrc.nist.gov) to map your existing documented controls to RS.CO subcategories. Build a simple control narrative document in a shared workspace (Google Docs, Confluence free tier) that maps each RS.CO subcategory to: (1) the control owner, (2) the evidence artifact (runbook, log sample, escalation ticket), and (3) the test date. For IR-4 specifically, attach the joint escalation protocol from Step 4 and a tabletop exercise record as evidence. This document is what you hand to a FINRA examiner asking how your cyber and fraud response functions coordinate.

**Evidence:** Before benchmarking, collect the artifacts that will populate the control narrative: prior examination findings or management response letters from FINRA that reference cybersecurity or fraud operations coordination (these define your regulatory baseline); results of any prior IR tabletop exercises, particularly whether ATO-to-fraud escalation was a scenario; and current policy documents for incident response and fraud investigations to identify where the two policies reference (or fail to reference) each other. The gap between what these artifacts show and what NIST CSF RS.CO requires is the precise scope of your remediation narrative.

## Detection Guidance

No IOCs are associated with this governance item. Detection guidance applies to the underlying threat techniques the fusion center is designed to address. For T1078 (Valid Accounts): monitor authentication logs for logins from new geographies, impossible travel events, or credential use outside business hours; correlate with downstream transaction activity. For T1566 (Phishing): review email gateway logs for lookalike domains and attachment types commonly used in BEC campaigns. For T1539 (Steal Web Session Cookie): monitor for session tokens used from IPs inconsistent with the authenticated user's history; short-lived token anomalies in web access logs are a primary indicator. For T1114 (Email Collection): alert on mail forwarding rule creation events in Microsoft 365 (AuditData EventSource: Exchange, Operation: New-InboxRule) or Google Workspace Admin logs. For T1657 (Financial Theft): correlate fraud case data with prior security events on the same account - this correlation is the core capability the fusion center is designed to enable.

## Framework Mappings

### MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1657** — Financial Theft
- **T1539** — Steal Web Session Cookie
- **T1114** — Email Collection

### NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)

### OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

**CIS-V8**

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **8.2** — Collect Audit Logs

**SOC2-TSC**

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

**HIPAA-SECURITY**

- **164.312(d)** — Person or Entity Authentication

**NIST-CSF-2**

- **DE.CM-01** — Networks and network services are monitored

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1078 | Valid Accounts | Defense-Evasion |
| T1566 | Phishing | Initial-Access |
| T1657 | Financial Theft | Impact |
| T1539 | Steal Web Session Cookie | Credential-Access |
| T1114 | Email Collection | Collection |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.darkreading.com/threat-intelligence/finra-launches-fina... | T3 |
| **In the context of a CVE, what does "unspecified vectors" mean?** | https://security.stackexchange.com/questions/82997/in-the-context-o... | T3 |
| **CWE-358: Improperly Implemented Security Check for Standard** | https://cwe.mitre.org/data/definitions/358.html | T3 |

| Source | URL | Tier |
|---|---|---|
| **Exploitable vs. Not-Exploitable: How to Tell the Difference for Your ...** | https://www.ox.security/blog/exploitable-vs-not-exploitable-can-you... | T3 |
| **An Ignored Vulnerability Counted as a Valid One** | https://community.blackduck.com/s/article/An-Ignored-vulnerability-... | T3 |



Generated 2026-04-10 18:37 UTC by TJS Security Command Center