Cooley

Senators Press FINRA on ACATS Fraud: What Broker-Dealers Should Do Now

August 24, 2026

On August 20, 2026, US Senators Ron Wyden and Elizabeth Warren sent a letter to FINRA President and CEO Robert W. Cook urging immediate regulatory action on fraud involving the Automated Customer Account Transfer Service (ACATS), the system used to move customer securities and cash between brokerage firms. The letter was also sent to Securities and Exchange Commission (SEC) Chairman Paul Atkins and Depository Trust & Clearing Corporation (DTCC) President and CEO Frank La Salla, underscoring that congressional concern extends beyond FINRA's direct regulatory perimeter. The letter identifies specific ACATS security gaps, names individual firms based on their current protections and calls for new rules on customer notification, transfer locks, transaction authentication and phishing-resistant multifactor authentication (MFA). FINRA must respond by September 17, 2026.

Although directed at FINRA rulemaking rather than any single firm, the letter signals where regulatory and reputational scrutiny is heading. Broker-dealers and other financial institutions handling ACATS transfers should assess their transfer-security controls, authentication practices and customer communications now rather than wait for a final rule.

The vulnerability

Administered by the US National Securities Clearing Corporation and governed by FINRA Rule 11870, ACATS gives an outgoing firm only one business day to validate or object to a transfer request and, if validated, three business days to complete it. The letter explains that this speed – designed to stop firms from obstructing customers who want to leave a brokerage firm – has created a gap: The outgoing firm does not need to notify or authenticate the actual account holder before a transfer proceeds. Fraudsters have exploited this gap by opening fraudulent accounts elsewhere using stolen information and pulling the victim's assets before the victim knows a transfer occurred. Wyden and Warren's letter cites an October 2025 New York Times investigation reporting on incidents at firms including Vanguard and Merrill.

Compounding the problem, the letter claims many firms do not reliably notify customers when a transfer is initiated. FINRA's Regulatory Notice 23-06, published in 2023, recommended but did not require such notification. The letter states that certain firms currently give no notice at all, eliminating the window customers would otherwise have to stop a fraudulent transfer.

Firm-by-firm findings

The letter reports firm-by-firm findings across multiple controls, including self-managed transfer-block features and support for phishing-resistant MFA, based on a review conducted by the senators' offices and direct outreach to major brokerages. The findings show substantial variation across the industry, with some firms offering robust, customer-controlled protections and others offering little or none.

Firms named in the letter should expect this level of public, comparative detail to be referenced in follow-on inquiries, press coverage or state regulatory attention, independent of what FINRA ultimately does with the rulemaking request.

What the letter asks FINRA to do

The letter's near-term request is to codify Regulatory Notice 23-06 into a binding rule requiring transfer notifications and a self-managed, opt-in transfer lock. Longer term, the request is to require verified outgoing-

holder confirmation via a dual-track framework, plus mandatory phishing-resistant MFA (passkeys), citing NIST SP 800-63 and 800-53, OMB M-22-09, and Japan's recent passkey mandate as a model.

Why it matters

Congressional letters of this kind do not themselves create binding legal obligations, and FINRA is not required to adopt any of the specific proposals described above. However, the letter is a meaningful signal for several reasons:

- It follows FINRA's own 2023 guidance identifying transfer notification as an "effective practice," meaning FINRA has already laid analytical groundwork that could support converting guidance into a rule.
- It references federal cybersecurity authentication standards (NIST SP 800-63 and 800-53, OMB M-22-09) that already exist and could be invoked in examinations, enforcement referrals or private litigation irrespective of a new FINRA rule.
- It creates a public record, firm by firm, of which institutions do and do not currently offer self-managed transfer locks and phishing-resistant MFA, which could be used by regulators or plaintiffs' counsel regardless of the rulemaking outcome.
- It highlights account-takeover and new-account fraud typologies that intersect with existing broker-dealer regulatory obligations, including Regulation S-P safeguarding requirements, SEC and FINRA Identity Theft Red Flags obligations under Regulation S-ID, FINRA Rules 3110 and 3120 supervisory obligations, and state data breach notification and safeguards laws that may be triggered if customer accounts are compromised.

Recommended actions

We recommend that broker-dealers and other financial institutions handling ACATS transfers take the following steps:

- Inventory ACATS transfer-lock controls and assess moving to a self-managed, customer-controlled model. Firms should evaluate whether they can deploy a comparable feature before any FINRA mandate.
- Confirm whether outbound transfer requests trigger customer notification, and if they do not, consider implementing a notification protocol.
- Benchmark MFA offerings against phishing-resistant standards (NIST SP 800-63 and 800-53, OMB M-22-09), with particular attention to passkey deployment.
- Review fraud-monitoring and escalation procedures for the account-opening/ACATS-pull typology described in Wyden and Warren's letter.
- Prepare for possible interest from regulators, plaintiffs' counsel and the media, including SEC examination inquiries, state attorney general and state securities regulator inquiries, and update board/risk-committee reporting as needed.
- Monitor FINRA's response, due September 17, 2026, and any resulting notice-and-comment rulemaking.

How we can help

Our cyber/data/privacy practice advises broker-dealers, banks, investment management firms and other financial institutions on FINRA and SEC cybersecurity and authentication obligations, incident response, and regulatory engagement. We can help benchmark your current controls against the protections highlighted in the letter, prepare for examination inquiries and, if useful, submit comments in any resulting FINRA rulemaking.

Key Contacts

Travis LeBlanc **Washington, DC**	**tleblanc@cooley.com** **+1 202 728 7018**
Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249
Michael La Marca New York	mlamarca@cooley.com +1 212 479 6132