United States Senate

WASHINGTON, DC 20510

August 20, 2026

Robert W. Cook
President and Chief Executive Officer
Financial Industry Regulatory Authority
1700 K Street, NW
Washington, DC 20006

Dear Mr. Cook:

We write to urge the Financial Industry Regulatory Authority (FINRA) to take immediate regulatory action to protect consumers from the growing threat of Automated Customer Account Transfer Service (ACATS) fraud.

ACATS is an automated system administered by the National Securities Clearing Corporation and regulated under FINRA Rule 11870, designed to allow investors to seamlessly transfer their stocks, bonds, and cash from one brokerage firm to another. Bad actors are increasingly exploiting structural weaknesses in the ACATS system to illicitly drain consumers' brokerage accounts, including retirement funds. While the speed of the current transfer process was originally designed to protect consumers by preventing anti-competitive behavior by brokerages, criminals are exploiting the complete lack of an outbound verification step by the account holder.

A recent review of major brokerage firms conducted by our offices reveals a deeply concerning lack of standardized, consumer-controlled protections across the industry. Only a few companies offer a way for consumers to protect their accounts. FINRA must protect consumers by modernizing its rules, establishing immediate requirements for notification of transfers and consumer-managed transfer locks in the short term, and requiring a secure process for consumers to approve outgoing transfers from their accounts in the longer term.

In the past, brokerage firms routinely dragged their feet to prevent consumers from transferring their assets to competitors who offered better rates or services. To eliminate these anti-competitive practices, regulators instituted strict, rapid timelines that exist to this day. Under current rules, the receiving brokerage firm initiates the transfer after receiving a request from the customer, leaving the outgoing brokerage firm with just one business day to either validate or object to the request. If validated, the outgoing brokerage firm must completely transfer the assets within three business days.

While this hyper-efficient timeline effectively solved a major consumer-protection issue of the past, it has inadvertently created a massive security vulnerability that fraudsters are exploiting. The ACATS system requires zero notification to or authentication from the actual account holder by the outgoing brokerage firm. Fraudsters exploit this by using stolen personal information to open a fraudulent account in a victim's name at a separate online brokerage and then submit an ACATS request to pull the victim’s life savings from their legitimate account. A New York Times investigation in October 2025 highlighted ACATS fraud incidents involving major brokerage firms like Vanguard and Merrill Lynch. These fraudulent account transfers occur entirely without the true account owner's knowledge or consent. The outgoing brokerage is legally bound by FINRA's rapid-turnaround mandates and the system does not prompt the true account owner to verify the transfer. As a result, assets are often swept away before the victim even realizes a transfer has been initiated.

Compounding this vulnerability is an even more basic breakdown in communication: the widespread failure to reliably notify consumers that a transfer is underway. In Regulatory Notice 23-06, published in March 2023, FINRA explicitly identified customer notification—via email, phone call, or mobile push notification—as an "effective practice" to mitigate the risks of fraudulent ACATS transfers. However, FINRA merely recommended this practice and did not require it. As a result, major financial institutions like Citi and Wells Fargo offer absolutely no notice or warning to their customers, stripping them of the vital three-day window to intervene and halt a fraudulent transfer before their assets are stolen.

An analysis conducted by our offices of leading brokerages confirms that security protocols are wildly inconsistent, leaving millions of retail investors needlessly exposed based solely on where they hold their assets. Fidelity and Vanguard offer an important industry model for customer protection by providing customers with fully self-managed ACATS transfer block features, while J.P. Morgan, Robinhood, Webull and Wells Fargo all indicated that they offer similar protections that can only be enabled or disabled by customer service. Following direct outreach from our offices, several brokerages have committed to offering protections for their customers. Webull and Robinhood have both agreed to upgrade their existing transfer blocks to a user-managed feature, by Q3 2026 and Q1 2027 respectively. Similarly, Interactive Brokers has committed to developing a self-service transfer lock, with an expected launch date of Q3 2026. Unfortunately, other major brokerage companies, including Citi, E*TRADE, Merrill Lynch (Bank of America) and Morgan Stanley Wealth Management do not offer similar mechanisms, which leaves their customers completely exposed to the vulnerable ACATS process. Charles Schwab similarly fails to offer ACATS transfer lock protection for its customers and has refused to provide written confirmation of future plans.

It is unacceptable that major brokerage firms are putting customers’ life savings at risk of being ripped off by criminals because of inadequate account protections. FINRA must step in to protect consumers. In the short term, FINRA must immediately codify the voluntary guidance from Regulatory Notice 23-06 into a binding rule that would require brokers to send text, email, or push alerts to account holders when an ACATS transfer request is received, several days before the customer's assets are transferred out of their account. FINRA should also require member broker-dealers to provide consumers with a self-managed, opt-in feature to safeguard their accounts against unauthorized transfers.

FINRA must also fundamentally modernize the ACATS process by requiring verified confirmation of the transfer by the outgoing account holder. To achieve this in a manner that protects all consumers, FINRA should mandate a dual-track authentication framework. For the vast majority of customers who manage their accounts online, FINRA must require that the transfer request be explicitly approved within an authenticated session on the outgoing broker's website or mobile application. Consumers already routinely log into their accounts to securely authorize access for third-party financial applications and services. Because most financial institutions already possess the capability to handle these secure verifications, extending similar protections to ACATS transfers should not require significant additional resources.

Crucially, to counter modern cyber threats, FINRA must also require brokers to secure customer accounts with phishing-resistant multi-factor authentication (MFA), specifically a technology called passkeys. Traditional MFA—such as verification codes sent by text message or email and mobile push notifications—can be easily bypassed by bad actors, which is why the National Institute of Standards and Technology Special Publications 800-63 and 800-53, alongside Office of Management and Budget Memorandum M-22-09, explicitly mandate phishing-resistant authentication.

Several brokerage companies already support passkeys, but do not require them—including Interactive Brokers, Merrill Lynch (Bank of America), Morgan Stanley Wealth Management, Robinhood, Vanguard, Webull and Wells Fargo. But these brokerages continue to support other, vulnerable methods of multi-factor authentication that do not meet federal cybersecurity standards. J.P. Morgan supports passkeys only for web-based account access, but not for its mobile app, while Fidelity—targeting September 2026—and E*TRADE are in the process of rolling out support. However, Charles Schwab and Citi lag behind, and only support insecure methods of multi-factor authentication that do not meet federal cybersecurity standards. Charles Schwab has refused to provide written confirmation of future plans.

While FINRA has yet to require that brokerages meet federal cybersecurity standards, financial regulators in Japan enacted rules requiring securities firms to mandate passkey-based authentication—not just to offer it as an option—for customer accounts by July 1, 2026. In response, Japanese brokerages have swiftly upgraded their customers' account security, proving that rapid, industry-wide adoption of modern cybersecurity technology is entirely achievable.

Finally, for the segment of consumers who do not manage their outgoing broker account online and therefore cannot digitally approve a transfer request, FINRA should require that the transfer application include a traditional Medallion Signature Guarantee, which requires an in-person trip to a financial institution, ensuring that offline and vulnerable investors are protected by an ironclad, verified paper trail before their life savings can be moved.

Please provide a response to this letter no later than September 17, 2026, detailing the steps that FINRA intends to take to protect investors.

Sincerely,

Ron Wyden
United States Senator

Elizabeth Warren
Ranking Member
Committee on Banking,
Housing, and Urban Affairs

CC: Paul Atkins, Chairman, U.S. Securities and Exchange Commission
Frank La Salla, President & CEO, Depository Trust & Clearing Corporation