

Petition for Rulemaking

Minimum Standards for Investment Participant Identity, Role, Authority, Classification, and Interoperable Verification

October 4, 2026

Secretary, U.S. Securities and Exchange Commission
100 F Street NE, Washington, DC 20549-1090

Dear Secretary:

Pursuant to Rule 192 of the Commission's Rules of Practice, Global Capital Institute LLC ("GCI") petitions the Securities and Exchange Commission to initiate rulemaking establishing mandatory minimum verification standards for investment participants and covered investment ecosystems within the Commission's jurisdiction.

The requested framework would require covered operators to verify relevant participant identity, organizational affiliation, role, authority, and classification; enable reusable credentials with expiration, renewal, and material-change controls; and maintain interoperable registers through which counterparties can check authenticity and current status. It would support prevention, detection, and evidence-based reporting of suspected investment fraud involving domestic or foreign actors.

1. Identity alone does not establish authority

Investment relationships require participants to understand whom a person represents, in what capacity they act, what authority they possess, and whether their classification is appropriate for the interaction. A real person may misrepresent an affiliation; an actual employee may lack authority to solicit capital; and a person claiming to be an investor may instead be acting as an intermediary.

Counterparties frequently must assemble this context from disconnected records, professional profiles, organizational websites, and participant statements. These proxies may support an inquiry without establishing the specific authority claimed. Repeated verification imposes costs on legitimate participants while gaps between systems give dishonest actors opportunities to reuse misleading claims.

The proposed framework would make essential claims independently checkable before sensitive information is shared, capital is committed, or reliance is placed on an investment solicitation. Its benefits should include more accurate matching and classification, less duplicative verification, and better access to legitimate capital relationships.

Existing availability through VerifyInvestor.com

IPD verification is already available through GCI's partner VerifyInvestor.com (Verify Investor, Inc.), a U.S.-based provider, at <https://www.verifyinvestor.com/gci-investment-role-designation>. Its existing review service provides a starting point for wider adoption; mandatory coverage and interoperable reporting are proposed extensions.

VerifyInvestor.com's parent company, tZERO, describes it as having likely built one of the largest U.S. databases of verified accredited investors. This database is distinct from participants who have completed IPD verification. Sources: VerifyInvestor.com's GCI designation page; tZERO's PandoAlts integration announcement.

2. Mandatory coverage across investment ecosystems

GCI requests that the Commission define covered activities and responsible operators so that minimum verification follows the investment relationship across environments. Coverage should include investment platforms and marketplaces, investment-focused events and networks, fundraising channels, and special purpose vehicles and their managers or sponsors, to the extent the relevant activities fall within SEC authority.

The obligation should attach to covered activity rather than the label, technology, or venue used. A move from a platform to an event, private group, or vehicle should not by itself remove the verification requirement. For activities outside SEC authority, GCI requests coordination with the appropriate authorities to explore compatible standards, rather than an assertion of jurisdiction the Commission does not possess.

Covered operators should require current verification before admitting a participant to relevant solicitation, representation, fundraising, or transaction functions. Verification should be proportionate to the role and activity. A prospective counterparty should be able to request that a solicitor obtain verification and check the result through an accessible status mechanism.

3. Minimum substantive requirements

Identity and affiliation. Establish the credential subject and substantiate organizational relationships, distinguishing employment, ownership, advisory capacity, and representation.

Role and authority. Record the capacity in which the participant acts and evidence supporting authority, with its organizational scope, relevant mandate, limitations, and validity period. A title or affiliation should not alone establish permission to act.

Classification. Apply controlled definitions to participant categories and preserve the basis of each conclusion. Independently checked facts, participant statements, and classifications derived under the standard must remain distinguishable.

Currency. Display review, issuance, and expiration dates; require periodic renewal; and provide correction, suspension, or revocation when authority, affiliation, or other material circumstances change. Scheduled renewal must not excuse ignoring a known intervening change.

Accountability. Preserve attributable review records, identify the verifier and credential issuer separately where appropriate, and establish correction, dispute, privacy, security, and oversight procedures.

Existing obligations. Receiving institutions retain applicable due diligence and compliance responsibilities. A profile classification is not automatically an accredited-investor determination, regulatory registration, transaction eligibility decision, or completion of KYC or another required procedure.

4. Interoperable registers and fraud prevention

GCI proposes a common information and status-checking framework connecting qualified verification providers, credential issuers, and covered ecosystem operators. Implementation could use approved APIs, secure exports, webhooks, embedded verification components, or equivalent methods. Common functions and interpretable claims, rather than a single proprietary technology, should determine interoperability.

A receiving system would authenticate the credential source, associate the credential with the correct presenter, identify the underlying verifier and governing standard version, interpret the claims and limitations, and check current status before relying on the credential. It would retain the identifier, relevant claims, status-check time, and action supported. Downstream transfers would preserve provenance, scope, and qualifications.

The register could be federated rather than a public repository of sensitive personal records. It should enable permitted checks of identity, role, authority, classification, and credential status while restricting access to underlying evidence. Corrections, expiration, withdrawal, and revocation should reach authorized relying systems through defined update procedures. An unavailable status check must not silently count as successful verification.

Mandatory adoption across covered environments would make it harder to evade verification by moving between platforms, events, or vehicles. Where lawfully permitted, consistent participant and entity references could help identify repeated attempts to use withdrawn credentials, false affiliations, unauthorized mandates, or inconsistent classifications. The system should distinguish an unverified claim or discrepancy from an established finding of misconduct.

5. Domestic and cross-border reporting

Covered operators should have procedures to preserve and refer credible evidence of suspected misconduct to the competent authority. A structured referral could include the relevant participant and entity references, claimed role or authority, verification history, observed discrepancy, interaction records, dates, affected parties, and evidence provenance. Reporting should use applicable SEC and other competent-authority channels and preserve any legally required confidentiality.

For foreign actors or cross-border activity, compatible records could support lawful coordination among U.S. authorities and their foreign counterparts. Sharing would remain subject to applicable privacy law, access restrictions, and authorized cooperation arrangements; it would not establish an unrestricted international blacklist or give private operators law-enforcement powers.

Risk alerts and credential actions should be evidence-based, auditable, and subject to correction and review. Nationality alone must not determine risk. Verification cannot guarantee that a participant will act lawfully, but it can make false claims harder to reuse and relevant evidence easier to connect and report.

6. GCI cooperation, IPD™, and TRUST STAR™

GCI has developed the IPD™ standard and protocols to structure verification of investment participant identity, role, authority, mandate, and relevant classification. GCI is willing to cooperate with the Commission, other competent authorities, and industry participants to incorporate its IPD standard and protocols into the development and implementation of the requested framework, including controlled definitions, verification outputs, renewal, status checking, and interoperability requirements.

GCI is also willing to make its TRUST STAR™ certification framework available to qualifying verification providers and participating platforms that meet the applicable GCI standards and protocols, subject to review, authorization, and continuing oversight. Certification would identify the approved scope of qualifying services or credential-use activities, rather than endorse every service offered by an organization.

GCI filed a U.S. certification mark application for TRUST STAR with the United States Patent and Trademark Office on September 24, 2026, under application serial number 50128561. The application is pending; this number is an application identifier, not a registration number. USPTO filing does not constitute regulatory approval of the verification framework.

Under GCI's framework, the underlying verifier remains accountable for its review; the credential issuer preserves the result's meaning and attribution; and the participating platform authenticates the credential, links it to the correct participant, and applies permitted claims within its approved workflow. Planned integration capabilities would not be represented as operational until delivered, tested, and approved.

The Commission's minimum requirements should remain provider-neutral. This petition does not request exclusive designation of GCI, compulsory purchase of IPD, or SEC endorsement of TRUST STAR. GCI offers its work as a practical contribution and potential implementation of common requirements.

7. Petitioner's interest and requested action

GCI is a self-funded public-purpose research and development firm. It owns and develops IPD and TRUST STAR and could benefit commercially from broader adoption. GCI discloses that interest and requests that the Commission assess the proposal on its public-interest merits, including fraud prevention, legitimate capital formation, interoperability, privacy, accessibility, and implementation costs.

GCI respectfully requests initiation of rulemaking and public comment on mandatory verification across covered investment ecosystems, reusable credentials and registers, and coordinated evidence-based reporting. Phased implementation and proportionate requirements should support smaller participants while preserving the substance of verification.

Respectfully submitted,

Tash Salas

Founder and President, Global Capital Institute LLC

1309 Coffeen Avenue, Suite 1200, Sheridan, WY 82801, United States

globalcapital.institute@gmail.com | <https://globalcapital.institute/>