Opacity

November 17, 2026

Via website submission

Vanessa A. Countryman, Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Re: Release No. 34-106402; File No. 4-927; How Tokenized Securities Can Reach Emerging-Market Investors from Within the US Regulatory Perimeter

Dear Ms. Countryman:

Opacity Labs supports the Commission's Innovation Exemption, which recognizes that distributed ledger technology can facilitate broader access to trading US securities. The exemption requires tokenized securities venues ("TSVs") to maintain their own eligibility rules, only admit permissioned wallets, and screen those wallets for sanctions, illicit finance and other relevant risks. For retail investors in emerging markets with small balances, the cost of meeting these obligations has historically made those accounts unprofitable to maintain.

This comment reproduces an article Opacity Labs published on October 17, 2026, at https://opacitylabs.com/newsroom/emerging-markets. The article explains why identity screening has priced emerging market investors out of US financial markets and services, and how upgrading identity verification lowers that cost. The article uses tokenized funds as its example, but the same mechanism applies more broadly to banks and brokerages. For a TSV operating under the Innovation Exemption, the mechanism offers a practical way to admit retail investors in emerging markets, while giving the sanctions and illicit finance screening better evidence to work with.

How Tokenization Finally Reaches Emerging Markets

Funds and banks turn away emerging-market investors because maintaining the accounts costs too much. Opacity lowers that cost to onboard the rest of the world.

Tokenization hasn't reached anyone new. BlackRock's $BUIDL carries a seven-figure minimum and Circle's $USYC a six-figure one. Meanwhile households in the emerging markets are moving savings into stablecoins to protect against local inflation.

A stablecoin issuer only verifies its direct counterparties and never learns who ends up holding the token. A tokenized money market fund doesn't get that luxury, since the issuer or its transfer agent has to know who holds every share. The difficulty in verifying the identity of any wallet explains the whole gap between the two products.

This poverty of verifiability is best documented in Treasury's 2023 de-risking report. US banks have spent a decade exiting categories of foreign customers, including remittance businesses and correspondent banks. The report named profitability, shaped by compliance costs, as the primary factor.

The emerging markets represent trillions of dollars in untapped capital. In order to facilitate their access to American financial markets and services, we must upgrade investor verification itself. That's what Opacity does.

Why maintaining accounts can be unprofitable

Take a nurse in Brazil who saves a few hundred dollars a month. An asset manager has several ways to structure a fund that could admit her today, and Circle's six-figure minimum on $USYC is a business decision, not a regulatory one. The reason no fund is open to the nurse is the operational cost over the entire life of the account.

A US firm can check a domestic customer against records it reaches directly, such as the credit bureaus and the registry behind the ID. Across a border those records sit within another jurisdiction, across systems that may not be reliable or available, so the firm falls back on documents the customer supplies and a person to review them.

What the firm receives is a photo of a passport and a PDF of a bank statement, sent by the person they describe from the other side of the planet, and both can be faked for the price of a software subscription. A human checking those documents is a black box. No one can replay whether the clerk caught the discrepancy on the third page or clicked through on a slow afternoon. Make the clerk perfect, honest and tireless, and a flawless judgment still leaves nothing the next firm can check against the source later.

This poverty of verifiability leaves the firm uncertain who it is dealing with, and uncertainty means manual supervision. The firm has to keep investigating doubts about who she is for as long as the account stays open, and there are always doubts. Her ID may have been copied in one of the breaches that happen every few months, and she may never have reported it. Ten years from now the firm still has to be able to show that the account belongs to the person who opened it. The fees generated on a few hundred dollars in savings a month do not pay for that, which is why firms refuse the category. So her savings stay in a stablecoin that never asked who she was.

How to upgrade identity verification

Opacity builds a digital credential from the holder's own internet accounts. She logs in to the ones she already has: a local bank, a university, a payroll system, a utility, a tax portal or the civil registry that issued her ID. Any account she can log in to can be a source, and the sources can be cross-referenced to check for consistency. The point is that these are the records the firm couldn't reach across the border. No data-sharing agreement, no registry integration and no cooperation from a foreign government is needed to get at them. All that's required is that the nurse can log in to the account from an ordinary web browser.

The technology is zkTLS. When she logs in, her browser already checks the site's TLS certificate to confirm it's talking to the real bank. zkTLS produces a proof of what that site showed her during the session, tied to that certificate, and the bank does no extra work. The proofs from separately kept records then have to agree: the civil registry supplies her name, date and place of birth, and the payroll and bank records show wages paid and received in that name. The records stay where they are. The credential carries the facts a firm needs plus proofs it can check for itself, which is what the clerk's judgment could never give the next firm.

One of the key benefits of this approach is the ease with which the credential can be refreshed. The nurse can log in to the same accounts later to prove she continues to have access, or connect new accounts that tell the same story. A passport is not required; without one she supplies more sources.

It's worth being precise about what is being upgraded here. Not the compliance rules, which stay the same, and not the firm's responsibility for them, which also stays the same. What changes is the evidence those rules run on. Today a firm that relies on anyone else's verification, a vendor, a correspondent bank, a fund's distributor, is taking on that party's judgment as its own operational risk and then paying to supervise it. The de-risking report documents where that leads: US banks dropped correspondent relationships because supervising another bank's clerks was more expensive than the relationships were worth. When the records behind a verification carry proofs that any party can check, supervision turns into verification. The firm still owns the obligation, but meeting it means checking proofs in software rather than auditing someone else's process by hand.

FinCEN and the federal banking regulators recently confirmed that electronic credentials can serve as one method of verifying a customer's identity where the bank's or credit union's customer-identification program permits. Their examples include digital certificates and verifiable digital credentials.

What changes for the fund

When the nurse's logins finish, the fund gets access to her credentials, with the source records and the proofs behind them, and nothing is waiting on a document review or a vendor. The fund applies the same identity checks, eligibility rules and risk screen as before, to better evidence.

Suppose the nurse is named Maria Silva, which is a common name, and a screening run flags a sanctions entry under it. Today the fund's compliance officer would be investigating a photographed ID that can't be rechecked at its source. With the credential, her civil registry record shows a different date and place of birth from the sanctions entry, the officer clears the match against that record, and the proof is kept for an examiner to re-verify. When the name is flagged again next year, a fresh proof lets the officer repeat the comparison in minutes instead of reopening the file. Less manual investigation is what supports a lower minimum.

The legal obligations do not change; only the method by which the investor supplies evidence does. The fund makes its own admission decision from the proofs in her credential, the transfer agent records her on the register once she is admitted, and a transfer to her completes only when her current credential meets the product's eligibility rules. Because the credential belongs to her rather than to the fund, the next product she wants to hold can read it too. That means a fund can admit savers who were never its customers without relying on another firm's verdict. Every investor who is verified once becomes a customer any product on the network can admit at the cost of checking her credential, so a pool of verified investors in a market is a distribution channel that didn't exist before. Issuers follow that pool, and each new product gives more savers a reason to get verified. The funds that help build the pool early are the ones it serves first.

Emerging markets have been treated as a risk category for a decade because the evidence about the people in them couldn't be checked. Once it can, they are a market like any other, and a large one.

Respectfully submitted,

Hersh Patel
hersh@opacitylabs.com
CEO and Co-Founder
Opacity Labs

Sources

- U.S. Department of the Treasury, *Treasury Department Announces 2023 De-Risking Strategy*, April 25, 2023. Supports profitability, shaped in part by compliance costs, as the primary driver of de-risking. https://home.treasury.gov/news/press-releases/jy1438
- FinCEN, jointly with the staffs of the Federal Reserve Board, FDIC, NCUA and OCC, *Frequently Asked Questions Regarding Treatment of Verifiable Digital Credentials Under the Customer Identification Program Rule*, September 8, 2026, Question 3. Confirms the use of electronic credentials under existing customer-identification requirements; the FAQs neither alter existing BSA legal or regulatory requirements nor establish new supervisory expectations. https://www.fincen.gov/system/files/2026-09/MDL-VDC-FAQs.pdf