From:	Mark Singleton
To:	Comments
Subject:	[EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)
Date:	Monday, September 15, 2025 9:11:51 AM

[redacted]

Ms. Jennifer M. Jones
Deputy Executive Secretary
Attention: Comments—RIN 3064-ZA49
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Dear Ms. Jones, Mr. McDonough, and Mr. Gould:

Re: Request for Information on Payments Fraud

Dear Mr. Gould, Mr. McDonough, and Ms. Jones,

I am Marvin E. (Mark) Singleton III, President & CEO of Citizens National Bank of Texas, a community bank serving Texans since 1868. For over 150 years, our bank has helped families, farmers, and small businesses in Ellis County and beyond, providing safe, reliable financial services rooted in accountability and trust.

Fraud across payments — whether checks, ACH, wires, or instant payments — has become one of the fastest-growing risks to the banking system. Yet the cause, and the solution, are not complicated. Fraud is always about following the money. Criminals look for the weakest point in the system that allows them to turn stolen or illicit funds into spendable cash. Today, that weakness is most often found at account opening. When institutions fail to properly verify new accounts, they hand criminals the keys to the system.

If every bank and fintech were required to consistently apply strong "Know Your Customer" standards at account opening, and if regulators enforced accountability when they did not, fraud levels would fall dramatically. This is not a call for new programs, new layers of regulation, or more red tape. It is a call to return to the fundamentals of banking: knowing who your customer is and standing behind the accounts you open.

At Citizens National Bank of Texas, we have invested heavily in protecting our customers in real time. We provide instant alerts and account updates that engage our customers the moment suspicious activity occurs. This partnership has significantly reduced our fraud losses and kept our customers better informed. But even with these efforts, we still see customers fall for scams — and, in some cases, become unwitting participants in fraud. This proves that no amount of education or real-time alerts alone can stop the problem. If criminals can still gain easy access to accounts at other institutions, they will continue to exploit the system and victimize consumers.

This dynamic is not unique to banking. Consider the example of copper theft. People steal copper from buildings and utilities because they know they can quickly sell it to scrap buyers who rarely ask

enough questions. Lawmakers could impose 15-year prison sentences for the thieves, but the smarter solution is to hold the buyers accountable. If scrap dealers were barred from buying stolen copper or required to meet rigorous verification standards, the theft would largely dry up.
Payments fraud operates the same way. The crime continues not because we lack laws, but because too many account "buyers" — banks, fintechs, and now crypto exchanges — fail to do their job of verifying who they are dealing with. The system rewards the thief because someone is always willing to buy what they're selling without asking hard questions.
Crypto is today's version of the scrap yard. It has become the notorious cash-out channel for ransomware and cyber-fraud. Criminals exploit crypto exchanges that allow accounts to be opened with inadequate verification or monitoring. Unless regulators insist that these channels are held to the same account-opening standards as banks, fraud will simply migrate to the weakest on-ramp.
The solution is straightforward and requires no new bureaucracy:

1. **Require enforceable account-opening standards across the board.** Every bank, fintech, and crypto exchange must meet the same strong KYC and CIP standards, with meaningful penalties for those who do not.
2. **Hold all institutions equally accountable.** Fraud is often enabled by the largest players who open accounts at scale with limited scrutiny. Community banks end up bearing the cost when fraudulent checks or transactions flow through the system. Accountability should not depend on size or market power.
3. **Preserve tools that work.** Regulation CC protections, reasonable funds-availability holds, and fraud return deadlines are not outdated burdens — they are essential tools to help banks detect and prevent fraud. Weakening them would only embolden criminals.
4. **Encourage real-time collaboration.** Secure, low-cost fraud-alert networks accessible to all banks, including community institutions, would help identify and shut down fraud pipelines more quickly.

At its core, fraud prevention is about discipline and accountability. Community banks like mine partner every day with our customers to protect them. But we cannot protect the system alone. Fraud has to be stopped at the front door, by holding every institution that opens accounts to the same high standard.
Thank you for the opportunity to comment. I urge the agencies to focus their efforts on following the money and enforcing account-opening discipline. If we cut off the easy cash-out points and hold every participant accountable, we will take the single most effective step possible toward reducing payments fraud and protecting consumers.
Sincerely,
/s/
Marvin E. (Mark) Singleton III
President & CEO
Citizens National Bank of Texas