From: Anji Burnham
To: Comments
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)
Date: Tuesday, September 16, 2025 6:06:39 PM

[redacted]

Jonathan Gould
Comptroller of the Currency, Office of the Comptroller of the Currency
Docket ID OCC-2025-0009

Benjamin W. McDonough
Deputy Secretary, Board of Governors of the Federal Reserve System
Docket No. OP-1866

Jennifer M. Jones
Deputy Executive Secretary, Federal Deposit Insurance Corporation
RIN 3064-ZA49

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

We are the BSA/AML Department of CorTrust Bank, a $1.5 billion community bank located in Mitchell, South Dakota. We are writing to respond to the Office of the Comptroller of the Currency (OCC)'s, Board of Governors of the Federal Reserve System (Board)'s, and Federal Deposit Insurance Corporation (FDIC)'s request for information (RFI) on payments fraud.

Since 1930, CorTrust Bank has been serving the needs of individuals and businesses throughout 16 South Dakota communities, and 15 Minnesota communities, with 37 branch locations. What started as a small operation assisting local farming families in Artesian, SD, has today grown into a fourth-generation family-owned community bank. From our humble beginnings, we've grown into a pillar of strength and stability, moving ahead through market swings and all of life's changes. As a community bank, we aren't driven by profits. We're driven by the desire to see our customers thrive. In fact, community banks:

- Represent $4.0 trillion in consumer, small business, and agricultural loans
- Employ nearly 700,000 people
- Make roughly 60% of U.S. small-business loans under $1 million and 80% of banking industry agricultural loans

When you work with CorTrust, you are supporting local small businesses, helping your neighborhood grow, and getting the personal attention you deserve.

Thank you to the agencies for issuing this RFI and seeking input on ways that the OCC, the Federal Reserve System (FRS), and the FDIC could take actions to help consumers, businesses, and financial institutions mitigate payments fraud. Community banks continue to

be challenged by a rise in fraud and scams across payment types, so agency action is much needed.

Specifically, the Bank has been affected by payments fraud in the following ways:

Online Account Takeover

Customers opened a HELOC and a checking account. Customers were receiving e-statements. HELOC and checking account not actively being used by the customer at the time of the fraud. Online banking was fraudulently created using the customer's information and a fraudulent email address and an unknown phone number. The fraudster transferred funds from the customer's HELOC to their checking account via online banking. Within a short period of time, checks cleared the checking account payable to individuals unknown to the customer. The fraudster had created check stock for our customer's account. Some ACH trials tried clearing the customer's checking account on behalf of a name unknown to the customer. This activity was confirmed fraud and was what alerted the bank of the other fraudulent activity in their account. The bank took a loss on this situation.

Business Email Compromise

Mortgage loan customer with the bank in the process of selling their property through a realtor. Title company responsible for the closing. Bank received an email from the title company requesting a payoff for the mortgage loan customer. Bank responded to the title company, quoting a payoff for the customer as of the closing date. Bank received an email from the title company questioning the payoff as they had received an "updated" payoff not matching the original payoff sent from the bank. It was determined by the bank the "updated" payoff was fraudulent using an incorrect amount and fraudulent wiring instructions. It was determined the realtor's email was compromised. The fraudulent wire was not sent, and no funds were lost in this compromise.

Wire Fraud stemming from a Business Email Compromise

Customer received an email from a familiar business. Attached to the email was an invoice for services rendered. Customer contacted the bank requesting to send an outgoing wire for the invoice referenced in the email from the business. The wiring instructions were listed at the bottom of the invoice. Customer's accounting team called the bank later in the day hoping to stop the wire request referenced above. They had realized customer's email was hacked and the entire exchange with the business was completely fabricated. The bank was able to stop the wire and no loss was taken. The bank helped the customer get dual control set up for outgoing wire requests going forward.

Customers were purchasing a school bus from a business they had used prior. Communication with the salesperson was being done through email. At some point, emails were compromised, and the payment method was changed from mailing a check to sending an ACH or wire. Fraudulent wire instructions were sent through the compromised emails, and the customer sent a large payment using the fraudulent wire instructions. A couple of weeks later, customer realized what happened when the actual salesperson reached out inquiring about not receiving a check in the mail. Funds were never recovered.

Wire Fraud

Customers were trying to purchase some large equipment online. They found a website they thought to be legit. They were instructed by the salesperson to make the purchase happen as soon as possible because the business was going to be closed for a week. Customer initiated a wire that day. A couple of weeks later, customer informed the bank they were scammed. It is believed the website was not legitimate. Customer took a loss with this fraudulent wire.

Check Fraud

A business customer had a large, altered check clear their account. The payee on the check was altered from a business to an individual. The dollar amount stayed the same. The check was in sequence making it hard for bank personnel/software to catch. Business customers notified the bank of the altered check within their time frame. The bank completed a Breach of Warranty Claim and sent it to the large financial institution involved but were denied. The bank suffered a large loss due to the bank's return windows being so much smaller than the customers.

Bank was alerted to a compromised check on customer's account. The check was reported by the Bank's fraud software as for sale on the dark web. A stop payment was placed on the check number to prevent it from posting to the customer's account. The check tried to clear customer's account in an altered state. The date and amount were the same but written in different handwriting. Customer confirmed the original check was mailed from the post office. No loss for the bank or customer.

Impersonation/Debit Card Fraud

Someone called into bank claiming to be a bank customer. The caller had all the customers' personal information and was able to increase the customers debit card limit and place a traveling customer notification on the account. A large amount of fraudulent debit card transactions occurred before the customer realized what was happening.

ACH Fraud

Bank had numerous PPP business loan customers fall victim to ACH Fraud. These customers were contacted by someone claiming to be with the bank's ACH department. Once on the phone, the impersonator would state there was fraud with the customers ACH Origination account and would ask for account credentials and security tokens. With that information, the impersonator was able to set up numerous ACH payments from our customer accounts.

Credit Card Fraud

The bank received faxes from a different financial institution requesting proof of authorization for payments being made on our bank customer's credit card. Upon review of the credit card account, bank identified 84 payments that had been made from same financial institution's account and applied to bank credit card customer. Due to the way these payments were made, bank could not prove authorization. Bank risk closed the credit card with a remaining balance to be paid over $15,000.00. The bank's credit card department has seen numerous cases such as this.

Romance Fraud

Customer met someone online and started an online romance. Shortly after, customer deposited a large fraudulent check that appeared to be drawn on her account at a different financial institution. Bank believes customer received the fraudulent check stock from the online boyfriend. Someone then called the bank claiming to be the customer. They were able to complete a traveling customer form on her behalf. This led to some large debit card transactions posting in Africa. Customer also withdrew a portion of the funds in cash. Once the cash was received, customer had a FEDEX charge. The next day, the check was returned as forged. Bank stopped a FEDEX package that supposedly contained an iPad for her boyfriend. Customer claimed she had already mailed the cash. She believed her boyfriend was going to bring her account current by mailing her some money orders and possibly coming to visit. Customer's account was written off and Bank has not received any payments.

Phishing Attack Against an Elderly Customer Involving Gift Cards and Crypto Activity

Customer received an Apple security warning. The warning instructed customer to use the contact information in the message if this was not a transaction he authorized. The phone number was listed. Customer called the number and was instructed to download an app to allow the scammer access to his computer. The scammer then instructed customer to log into his online banking where the scammer was able to misrepresent customer's account balances. This led customer to believe he owed the scammer money and needed to pay them back right away. Customer came to the bank to withdraw cash. He told bank staff he was doing a home remodel and was getting a discount for paying in cash. The scammer then instructed customer on how to "return" the funds. Customer purchased two Apple gift cards and sent pictures to the scammer with the codes. Customer was then instructed to send funds via Western Union through Walmart. He was told to tell the cashier it was for a neighbor who moved to Argentina and needed help with medical bills. With the remaining funds, customer was instructed to put into a Bitcoin machine. Customer realized the scam when he could no longer reach the fraudsters and then checked his accounts via online banking. The customer had been scammed out of his life's savings. Devastating loss for the customer. The majority of situations brought to our attention involving Bitcoin are fraudulent.

Pigbutchering Fraud

Customer started having PayPal and Cash App activity in their account. There are numerous transactions being declined on the debit card as they exceed the customer's limits. The customers started withdrawing large amounts of cash from the bank. The only comment they made at the time of the withdrawals was they never splurge, so they are going to have fun. Customers have also sent funds to Bitcoin by ACH. Customer shared they are talking to Elon Musk. Customer mentioned they sent this individual $50,000 with the belief they were investing their money. They also said they were instructed to log onto an application where they could see the balance in their account growing. Customers believed they were going to receive a $500,000 check in the mail soon. When customer questioned the scammer on the application, the application went down, and she has not been able to log in since. Customers were told to send all their bank and credit card statements to help assist in getting the application back up. They did not send these documents. Customers suffered a large loss in this scam.

External Collaboration

The Bank supports collaborative stakeholder efforts to address payments fraud. Fraud and scams persist across state borders, so national stakeholder collaboration is necessary to effectively combat the problem. However, national efforts must recognize the resource constraints individual community banks face when deciding whether to participate.

Local and regional collaboration across community banks, federal and state regulators, law enforcement, community organizations, and other stakeholders can be an effective way to build connections and share information at the community level.

Consumer, Business, and Industry Education

Community banks thrive, in part, because of their close customer relationships. In-branch material and messaging are especially valuable for community banks. CorTrust Bank has created brochures and flyers to help educate our customers on potential scams and fraudulent activity. We also send out a quarterly email to our customers with current up-to-date information on educational topics. We have also partnered with AARP in the past to help with our fraud education.

Community banks serve elderly customers, as well as consumers and small businesses in rural and agricultural areas, so educational materials tailored to these groups would be valuable. Our CorClub meets periodically and education on fraud and scams is typically on the agenda. Any material created and shared on these important topics would be valued.

Regulation and Supervision

Broadly speaking, payments fraud regulations and examiner expectations need to be appropriately tailored to community banks with tiered compliance requirements and deadlines. There are opportunities to enhance supervisory guidance around appropriate controls, suitable technology, reporting, and incident response, but it is important to avoid imposing new burdens on community banks.

Check fraud remains a significant issue. Community banks are concerned some large financial institutions are not exercising sufficient CIP/KYC processes and opening accounts being leveraged by fraudsters. Similarly, community banks have had significant difficulty resolving interbank disputes regarding fraudulent checks. We are noticing large brokerage firm communication and CIP/KYC processes are also inefficient. Here's some examples:

- Customer disputed a check clearing their account. It was altered. Bank e-mailed large financial institution three times within four months and sent a fax. Large financial institution then rejected the dispute as a "counterfeit item" after twelve months. Customer bank then e-mailed again stating it was not counterfeit. It was an altered item. Denial letter was received one month later.
- Large financial institution was e-mailed by customer bank February 2025 about a check deposited by their customer on our bank customer's account that was written to someone other than the intended recipient. No response received to-date.
- In May 2025, bank customer disputed an altered check. Customer's bank emailed the large financial institution. No response to-date.

In June 2025, bank customer reported a stolen check. The intended recipient did not receive the funds. The check was then presented at a large institution. Customer bank e-mailed the large financial institution and have not received a response to-date.

- Bank customers were planning a vacation with friends. Friends banked elsewhere but they were all using the same travel company. Customers initiated a wire to the travel agent for their trip. A few hours later, customer called to cancel the wire as their friends were no longer able to reach the travel company once they sent the wires. It was confirmed fraud by the travel agent. Bank sent a recall to the large financial institution that received the wire. The institution requested a hold harmless and reason for the recall. Bank completed the request the same day and sent it to the larger institution. The large financial institution said it could take up to 90 days to process. Bank sent correspondence for updates, but the large institution stopped responding. 90 days has long passed, and the funds were never returned by the large institution.

Changes to Regulation CC could help community banks prevent and mitigate check fraud. The return deadline related to fraud could be extended, the "reasonable cause to doubt collectability" exception could be clarified, and relevant definitions could be revised. However, hold times should not be shortened; they are an essential tool for banks to detect and prevent check fraud. Financial institutions should have flexibility to extend hold times under appropriate circumstances. Also, holds on Cashier's Checks to be extended longer than next day.

Payments Fraud Data Collection and Information Sharing

While centralized data reporting would be valuable for the ecosystem, agencies should avoid imposing additional data collection requirements on community banks. Appropriate safe harbors would improve banks' ability and willingness to share fraud data.

Community banks would benefit from automated data collection, analysis, and reporting tools integrated with services they already use and do not come with additional costs.

Reserve Banks' Operator Tools and Services

Community banks would benefit from tools and services that integrate with third-party services they already use and pricing that is appropriate for their size and complexity. We currently use a BSA/AML fraud and detection product. While it's a great resource, it's expensive. Community banks are highly recommended to have a BSA/AML product to risk rate their customers, but the cost of doing so is an issue and at times discourages banks from getting the best product for their needs.

There are a variety of specific products and services that could benefit community banks, including, for example, a fraud contact directory, a fraud information sharing repository, an interbank check fraud breach of warranty claim mechanism, a check image analysis and verification tool, an atypical payment monitoring service, and confirmation of payee service.

General Questions

We have seen several types of fraud including Online Account Takeover, Check, ACH, Wire, Deposit, Crypto, Gift Card, Credit Card and Debit Card. We also have seen Elder/Dependent Abuse and Romance Scams. Identity Theft is also prevalent currently. We are seeing an uptick in phishing email situations and tech support scams such as pop-ups on the computer screen and fake security warnings.

We utilize the Nasdaq Verafin system to help with fraud detection, AML/CFT compliance and high-risk customer management. We also recently activated the Q6 Cyber product for fraud prevention. This product monitors the digital underground, dark web and private messaging apps. We highly recommend customers utilize our ACH Filter and Positive Pay products for fraud detection. We have our CaseTracker program on our debit cards scoring every transaction attempted/made on a debit card for potential fraud situations. SecureNow is utilized for our online/mobile banking sending a code to the customer if an unregistered device is used. Also, on online/mobile banking, alert management is encouraged on the site. We have added a questionnaire to be completed with every wire request. A Be Aware brochure has been created to read or hand out to customers with potential fraud situations alerting them of red flags. ACH's less or equal to $1 are monitored daily for fraudulent ACH trials in customer accounts. Also, training is being conducted on fraud at every level in the bank continuously.

Thank you for the opportunity to provide comments on this RFI. The Bank looks forward to continuing to work with the OCC, FRS, and FDIC, and other stakeholders to protect our customers and communities from the growing threat of payments fraud.

Sincerely,
/s/
CorTrust Bank N.A.