A Proud Past – A Promising Future

McLean County

STATE OF NORTH DAKOTA

712 5th Avenue
P.O. Box 1108
Washburn, ND 58577-1108
Phone: 701.462.8541
Fax: 701.462.8212
www.mcleancountynd.gov
Service: 28sa@nd.gov

Ladd R. Erickson
McLean County State's Attorney

Karissa K. Rittenbach, Legal Assistant
krittenbach@nd.gov; 701.462.8833
Kelsey J. Renner, Legal Secretary
kjrenner@nd.gov; 701.462.8832

March 10, 2025

Mr. Chairman and members of the committee:

My name is Ladd Erickson and I am the McLean County State's attorney. I support HB1447, but would suggest the Committee revisit some amendments the House put into the original bill that inadvertently facilitates crypto currency scams instead of protecting people from them. Specifically, Section 5 of the engrossed bill, as I will explain in my oral testimony.

Pig butchering schemes often start with solicitations of modest investments intended to bolster your confidence. They usually involve some type of fake claim or falsified dashboard that shows assets exponentially growing, with the intent being to encourage larger and larger investments.

A Slow Build

Here's how pig butchering investment schemes frequently work: A stranger will contact you out of the blue via text message, on social media or on a messaging application such as WhatsApp or WeChat and attempt to build rapport. They might provide an unusual explanation for why they're contacting you, such as having found your name in their contacts list, and often have online profiles that include fake but realistic-looking photos intended to pique your interest. They might also come across as wanting to develop a genuine friendship or romantic relationship.

Over the course of days, weeks or even months, the fraudster will send you messages about personal, non-investment-related topics. They might try to foster trust by sending pictures, talking about activities—such as volunteering—to demonstrate good character, or sharing fictitious life details that mirror your own. They might claim to be a widow, a single parent or even a member of the U.S. military living overseas, for example. In the process, the fraudster will also seek to obtain information that they can later use to manipulate you into surrendering your money.

Though these scams can present in different ways, inevitably the scammer will at some point steer the conversation toward investment-related topics, often asking whether you have an investment or crypto account.

Sharpening the Knife

The goals for the next phase of the scheme are twofold: to create the perception that you'll make money by following the bad actor's instructions and to ensure that you have the ability to invest into the forthcoming scam.

In one common scenario, for example, a fraudster might share that they have a connection at a reputable financial institution who gives lucrative investment advice and offer to share that advice with you. They might send screenshots of their

alleged brokerage account to demonstrate investment gains from the connection's prior stock picks. After you express a willingness to invest, the bad actor might ask you to verify that your brokerage account has the ability to trade in the relevant security, then provide additional instructions, including the company to invest in, the specific quantity to purchase and a specific price. They'll typically claim that you need to place an order to buy the stock immediately and might also ask you to send a screenshot proving that you executed the trade.

In another common scenario, the bad actor will dangle riches supposedly made through trading cryptocurrency. After gaining your trust, they'll encourage you to purchase or transfer cryptocurrency assets using a specific trading platform, which is likely to be fake and controlled by the scammer or their associates.

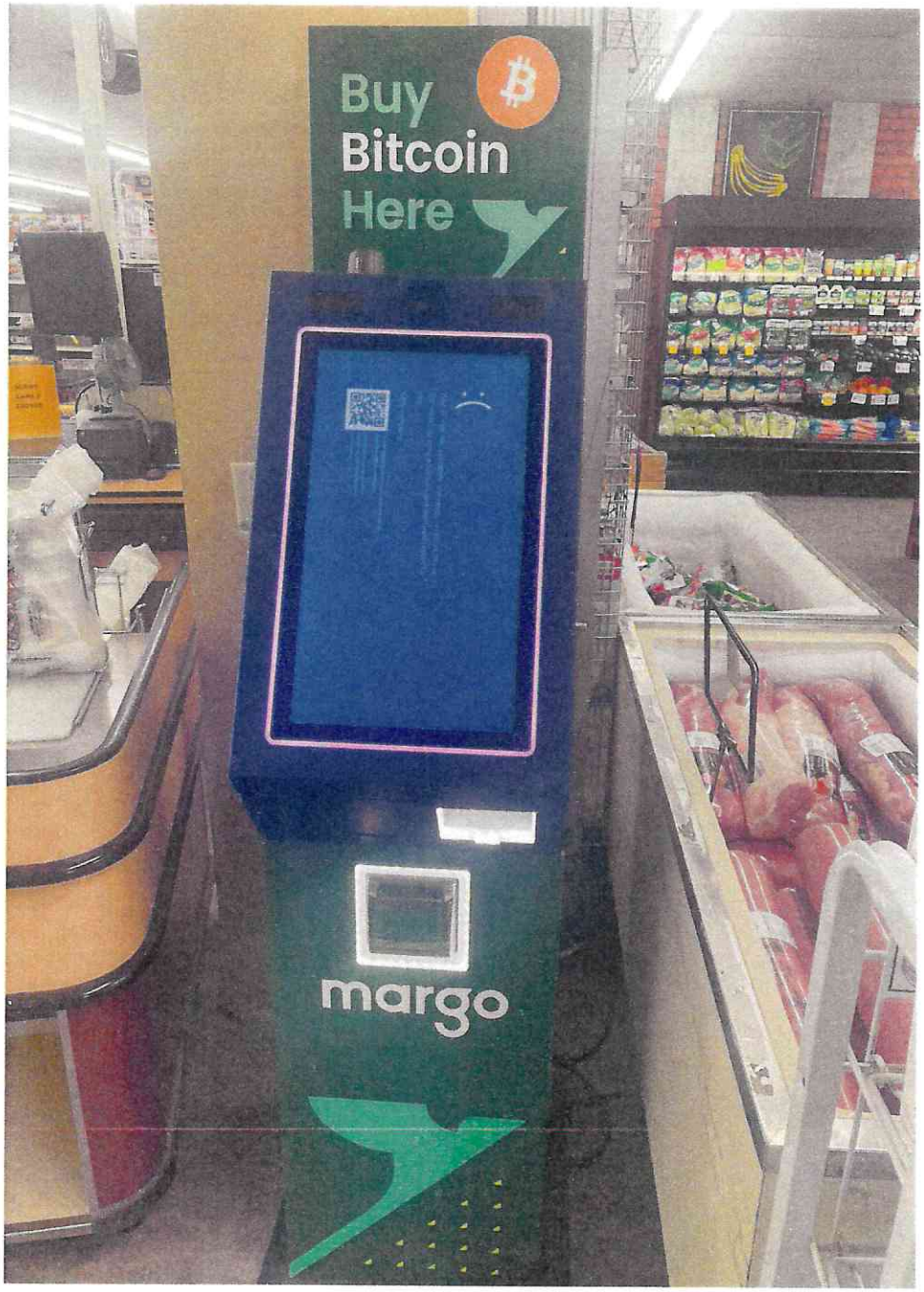
Other variations of these scams have the same goal: Entice you to put your money toward the "opportunity" they've shared.

It's important to realize that, while you might be executing such trades in your own investment accounts and with your own funds, the fraudster might be manipulating your decision-making in these and other pig butchering scenarios.

The Slaughter

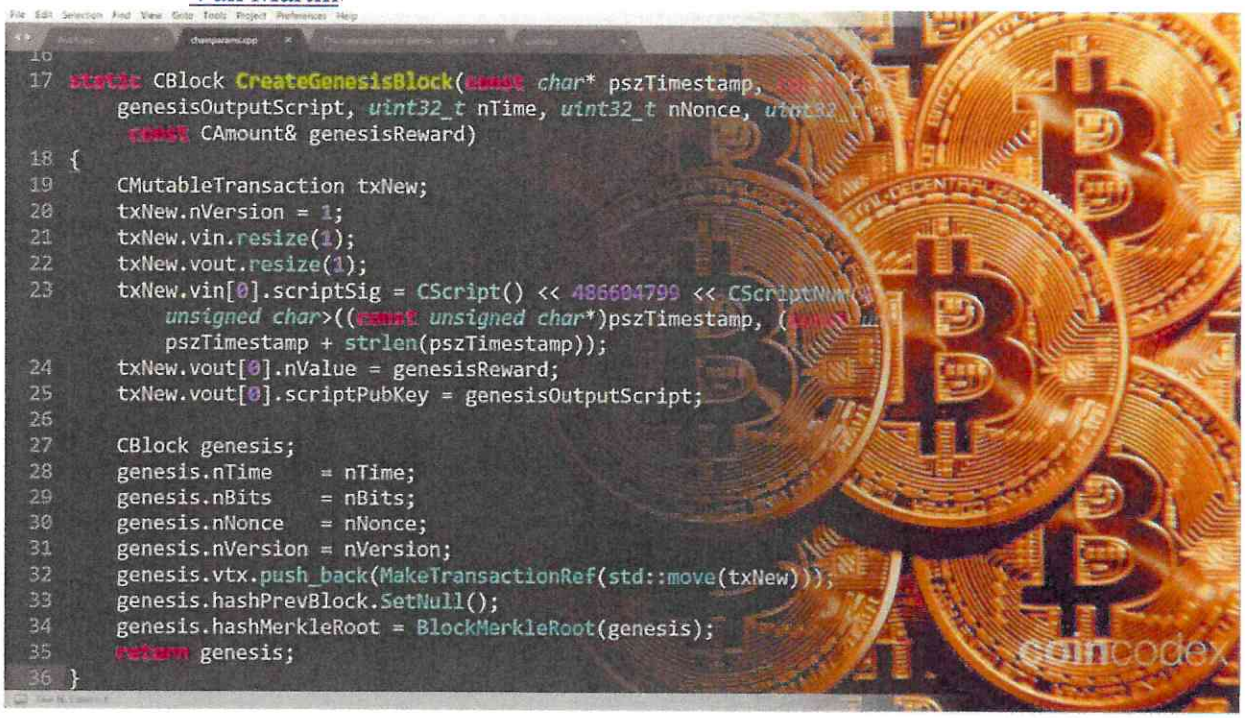
Capitalizing on the relationship they've established with you, scammers will point to impressive gains from initial investments and urge you to deposit increasingly larger amounts. Once you do, however, the switch will flip, often leaving you facing devastating losses. The price of a stock that seemed poised to take off might rapidly plummet once the scammer's market manipulation kicks into high gear. Or the new crypto platform you recently moved your assets into might suddenly become inaccessible.

If you confront the bad actor regarding the losses, they might express empathy and offer to help you recover your money, perhaps attempting to persuade you to invest in another stock. They might cite additional taxes and fees that you must pay before withdrawing your funds, especially if the investment scam involved crypto assets. And sometimes the bad actor will ghost you once the investment goes south.


Buy
Bitcoin
Here
margo

Bitcoin is 77,000 lines of computer code.

Vuk Martin



BLOCKCHAIN

COLUMN A	COLUMN B
LADD	10 (Bitcoin)

Owner Applied Number		Bicycle Make	
Finish		Bicycle Model	
Condition		Bicycle Speed	
Identifying Marks		Bicycle Wheel Size	
Recovered Date		Color	
Owner	[redacted]		
Disposition		Boat Name	
Evidence Tag		Boat Type	
		HIN	
Color Type	Color	Hull Shape	
		Propulsion	
Vehicle Type		Boat Length	
Vehicle Year			
Odometer Reading		Drug Type	
Body Style		Drug Quantity	
License Number		Drug Measure	
License Exp. Date			
License State		Notes	135.88 in charges from 6-4-2022 to 6-7-2022. Capital one card ending in #[redacted] belonging [redacted].

Narrative

6/10/2022 12:00:00 AM	4427 - Matties, Aaron R

On this above date, I spoke with a [redacted] lives in Butte, North Dakota. [redacted] stated that last week in between May 31 and June 2nd that her computer locked-up and a number popped up on her screen to get it fixed. [redacted] stated that it was a "Microsoft Number" and that a phone number came up to call. The phone number 909-550-6296 was the number that was on her computer to call to fix the shutdown. [redacted] called the number and thought it was Microsoft. The person from "Microsoft" got some information from [redacted] entered a passcode into a box on her computer. This included where she banked at, and they stated that her accounts may have been hacked. [redacted] stated that they transferred her to Bremer Bank, Minneapolis, Minnesota and she spoke to Rick Harrison of Bremer Bank.

[redacted] stated that Mr. Harrison showed her columns on her computer, and that there was three columns, and there was writing and numbers in the columns. Mr. Harrison stated to her that those should be blank, and that there were scammers trying to get her money out of Bremer Bank. [redacted] was told that she needed to first remove her money from the bank, and get it secured into a different account. Mr. Harrison obtained her phone number from her and told her to go to the bank. Mr. Harrison gave her directions to Dakota Square Mall, to Crypto currency kiosk in Minot, North Dakota. Mr. Harrison informed her that what she needed to do was to put all of the money into a wallet. [redacted] stated that she received these "phone scans" on her phone from Mr. Harrison. She then deposited money using her driver's license into a dark web crypto currency account. She deposited money total of $10,562 dollars on 06/02/2022. [redacted] then transferred $5,059 into the same cryptocurrency kiosk on 6/3/2022. [redacted] bought "Litecoin" and "Dogecoin" during the transactions. There was also scan codes that I took pictures of. [redacted] kept telling me that

this is how she would keep her money safe from the scammers that hacked into her computer. [redacted] told me that her computer didn't work the next day, and was still locked up. [redacted] was told to continue to put more money into a Crypto Wallet to keep her money safe. [redacted] deposited more money into a Crypto Wallet on 6-7-2022 at a kiosk in Mandan, North Dakota. [redacted] deposited four deposits $1600, 3700, 7,400, 300, into crpro currency wallets that Rick Harrison told her to put them in.

On 6-7-2022 I received a call from a Tad Pritchett of Morton County Sheriff's Department. Deputy Pritchett was in a store in Mandan, North Dakota Barney's 3.1 on 6th and Main Street, and workers told him about a lady that was shoving money into a crypto currency machine and was on the phone. Officer Pritchett stated to me that he talked to a lady named [redacted], and asked her if she was OK. [redacted] told the officer that she was helping her son [redacted] in California with investing money into crypto currency, and was on the phone with him. Officer Pritchett told me that he spoke with the person on the phone, who identified himself as [redacted], son of [redacted]. Officer [redacted] said that the man had an accent, and he asked [redacted] if her son had an accent. [redacted] stated that it was her son. I asked [redacted] about this when I took the report, and she stated that [redacted] told her do this. I asked [redacted], didn't she think this was weird, and a scam, and she stated that it just didn't come to her at the moment. [redacted] went back home, and her computer was fixed.

[redacted] stated that she spoke with people personally at Bremer Bank in Minot, North Dakota. [redacted] was given information on scams, and received password protection on her accounts, and more security on her accounts. [redacted] stated to me that Bremer Bank checked and that they don't have a Rick Harrison working for them at any Bremer Bank. [redacted] had a total loss of $28,621 for all her deposits to the Kiosks.

On 6-14-2022, I spoke with [redacted] about her Capital One Bank Account. [redacted] told me that she had charges that she didn't authorize to her Capital One Credit Card for $135.88 total, and they were four different charges. Deputy Paul Barrette met with [redacted] at her residence in rural Butte, North Dakota, and provided picture copies of the account charges.

Charges were these:
6-03-2022-Probiller.com $130.79
06-03-2022-Probiller.com $1.09
6-6-2022-ecst.net$2.00
6-7-2022-vxnbill.com-$2.00

[redacted] stated that her card was protected and she was credited with her money back on the account. I explained to about her money, and about the "Dark Web." I told [redacted] that her money is from the crpto currency is so hard to trace and that she will not be able to get her money back. I told her to call Bremer Bank and ask them if she would have any account protection to get her money back. I gave [redacted] my card, and told her if she had any questions to call me.

End of Report, 4427

Please see Deputy Pritchett's report in sheriff's data

Evidence Checklist

Additional Evidence Items?

Video Recording
In-Car Video
Surveillance
Interview Room
Other Recording
What other recordings are there?