'Pig Butchering': The Scam That Exploits Crypto Confusion

By **Brandon Essig and Mary Parrish McCracken** (September 5, 2024)

Brandon Essig

Mary Parrish McCracken

It starts with a seemingly ordinary but unsolicited text message or direct message from an unknown number or user. Maybe the sender has an attractive profile picture, and perhaps they demonstrate some pleasant, good-natured confusion at the phone number mix-up. But alarming trends tell us that, in all likelihood, it is not an accident but the genesis of a dangerous — and effective — online scam.

The technique is called "pig butchering," and just as the name grotesquely suggests, it alludes to the fattening of a hog before slaughter. And with the scam's increasing popularity, financial institutions now need to take action against exploitation or risk liability.

The victims are referred to as "pigs" by scammers, who assume false identities and tell elaborate stories intended to lure their victims into trusted online relationships and sometimes even romances.

Having gained the confidence of their victim, the scammers parade themselves as wealthy, having built fortunes through their crypto expertise — "expertise" that they then use to "help" their victims invest money into accounts on fake crypto exchanges.

Over the course of months, the victims fatten their online accounts, and like in a Ponzi scheme, the scammers steal more and more of the victim's money. Once the victims cannot or will not deposit more, they lose access to their investments.

They are then informed that the only way to retrieve their cash is by depositing even more money or paying a hefty fee. To state the obvious, any additional funds disappear, too.

The financial loss can be significant — researchers at the University of Texas estimate as much as $75 billion has been lost to the crypto scam[1] — and the realization that one's money has disappeared is a devastating and enduring "slaughtering."

What sets the scam apart and contributes to its success is its relative sophistication. The crime is perpetrated by enterprise-level syndicates that are supported by armies of South Asian laborers, often themselves victims of human trafficking. Fraudulent job ads lure individuals into working in Cambodia, Laos or Myanmar, among others, where they are stripped of their passports and trapped in scam compounds.[2]

Those who do not agree to become fraudsters could face beatings and other forms of abuse. Others accept their unfortunate fate as cybercriminals.

The syndicates these cybercriminals work for, by now, know what works. That is to say, the scammers leverage social engineering tactics and legitimate tools to build relationships and inspire a false sense of confidence.

For one, scammers are known to use AI-generated profile photos or photoshopped images to avoid any reverse image search hits, and in some cases, have been known to conduct

video calls with scam victims using AI software.

Scammers often begin by building a financial and personal profile of the victims they are targeting — they prefer victims with titles and higher net worths and those who may be lonely and thus more willing to engage with them.

Then, to win the trust of their victims, flim-flam scammers provide instructions for purchasing crypto-stable coins on well-known crypto exchanges. It is then, as the thinking goes, easier for the scammer to persuade their victim to transfer funds to fake trading apps that look and sound legitimate to crypto newbies.

The key for the scammers is to convey legitimacy and a false sense of security. The interfaces of these fake trading apps — which can often be downloaded from app stores — are set up to have the look, detail and functionality of a real trading app. Some scammers use legitimate software that allows anyone to build a trading platform, or they use clones of well-known trading apps, which are modified to simulate transactions to convince the victims that real trades are happening.

Some of the scam brokers have fake help desks to field phone calls, and they encourage the use of features like two-factor authentication. Most alarmingly, some of the sites are even registered with the U.S. Securities and Exchange Commission.

In short, the scam exploits not only their victims' emotions but also their crypto confusion. The collapse of Heartland Tri-State Bank is only one example proving that even professionals and executives are vulnerable to these schemes.

In May, the bank's former CEO, Shan Hanes, pled guilty in USA v. Hanes in the U.S. District Court for the District of Kansas to embezzling $47 million of the bank's funds that he wired to cryptocurrency accounts controlled by scammers, becoming one of the more notorious victims of a pig butchering scam**.**

In 2022, a cybercriminal contacted Hanes through WhatsApp, convincing him of a promising, too-good-to-be-true investment opportunity in cryptocurrency. By leveraging emotional appeals to Hanes' greed, scammers manipulated him into wiring first his own funds, and then stolen funds, into fake crypto accounts, and Hanes continued to believe the scam was real until he was arrested.

Hanes never realized any profit and lost all of the money he stole, and his conduct ultimately led to the bank's collapse and subsequent shutdown in 2023. He was sentenced to 24 years in prison after pleading guilty to one count of embezzlement.

What originated in China is now going global. Due to the scam's online medium, it has flourished during the pandemic, and as operations are gravitating into the U.S., law enforcement and regulators are beginning to take notice.

The FBI issued a warning about pig butchering in February, and prosecutors are beginning to initiate the freezing of crypto wallets associated with scammers masquerading as internet friends and seizing websites believed to be involved in the conduct.

At the state level, securities regulation agencies are issuing cease-and-desist orders to fraudulent cryptocurrency investment sites MetaCapitals Ltd., Cresttrademining Ltd., Forex Market Trade, and BATCNAP, among others, for the sale of unregistered securities.

But for now, the response is neither unified nor full-throated, prompting the U.S. Commodity Futures Trading Commission and the U.S. Department of Justice cryptocurrency enforcement team to convene a new working group for the coordination of efforts to stamp out these schemes at their root.

Still, as law enforcement works to catch up, the popularity of the scam continues to rise, and now, the ineffective whack-a-mole approach to combating it demands the attention of financial institutions, which up to now have similarly been lax in their approach to monitoring and disrupting this criminal activity.

The Financial Crimes Enforcement Network has recognized as much. According to FinCEN, financial institutions should be putting themselves in positions to recognize behavioral, financial and technical red flags that make it possible to suss out whether their customers may be falling prey to cybercriminals.

Alarm bells should be going off in the following examples:

- If a customer begins exchanging fiat currency for virtual currency despite no history of interaction with virtual currency;
- If a customer shows concern about their ability to access funds;
- If they mention having been instructed to exchange fiat currency for virtual currency; and
- If the customer mentions an investment opportunity that they learned about from a new contact or "friend."

FinCEN's Sept. 8, 2023, alert says that other financial and technical activity can be telling, too.

Customers who liquidate their savings accounts before maturation, who take out additional mortgages or lines of credit on their homes to purchase virtual currency, or who receive deposits of virtual currency at or slightly above the amount that was previously transferred out of their virtual currency account may be exhibiting financial activity suggesting they are becoming or have already become a "pig."

Banks can also view logs showing technical activity, including access to customer accounts by unique IP addresses, device IDs or new locations, to monitor suspicious activity akin to pig butchering.

These red flags can and should be a learning opportunity and provide a road map for financial institutions, which are in the best position to monitor entry points into the crypto space, detect suspicious activity, and at the bottom, provide a necessary backstop for vulnerable customers.

More importantly, the engagement of financial institutions is becoming the vital front-line approach to effectively tracking the flow of criminal proceeds, which are often impossible to recover, and prevent scammers from accessing those stolen funds.

Indeed, scammers may not want to fatten pigs if there is nothing to eat.

Brandon K. Essig is a partner and Mary Parrish McCracken is an associate at Lightfoot

Franklin & White LLC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4742235.

[2] https://www.icba.org/newsroom/blogs/main-street-matters/2024/04/11/pig-butchering-crypto-scams-a-growing-concern.