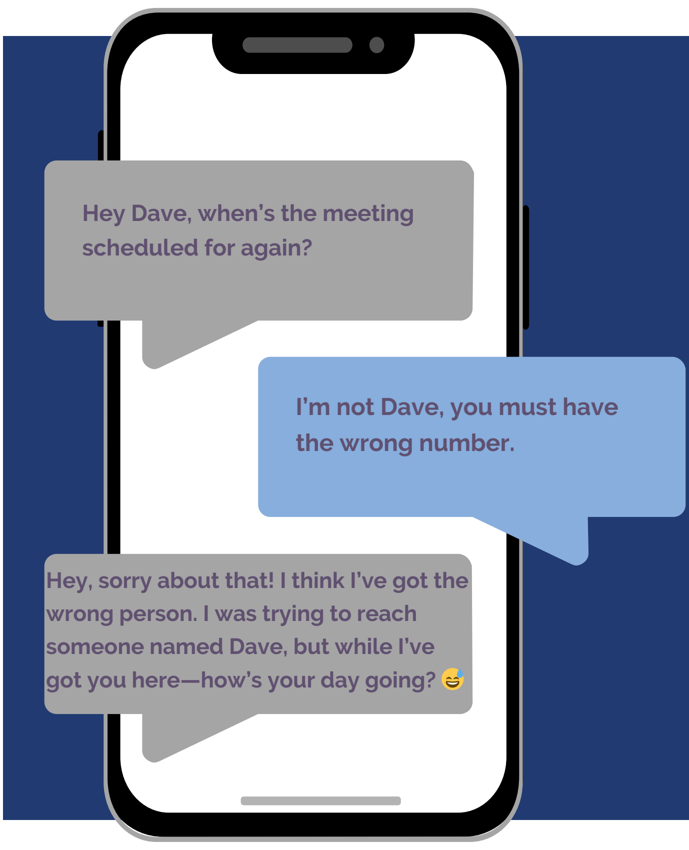
DFPI DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION

PROTECTING CONSUMERS
FOSTERING TRUST & INNOVATION
www.DFPI.ca.gov

Pig Butchering Scam Playbook

What are Pig Butchering Scams?

Pig butchering scams are a form of investment fraud in the crypto space where scammers build relationships with targets through social engineering and then lure them to invest crypto in fake opportunities or platforms created by the scammer. These scams often start with casual outreach via text messages, dating apps, or social media/messaging platforms to engage individuals.



Hey Dave, when's the meeting scheduled for again?

I'm not Dave, you must have the wrong number.

Hey, sorry about that! I think I've got the wrong person. I was trying to reach someone named Dave, but while I've got you here—how's your day going? 😅

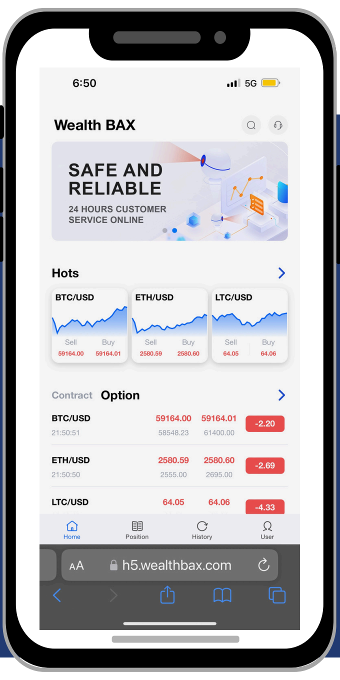
These text messages may seem harmless, but they are designed to start a conversation that leads to ongoing communication. Scammers are trained to use a variety of conversation techniques (e.g. feign romantic interest, mirror shared hobbies) to gradually develop a relationship with their target and gain their confidence. Scammers can spend weeks, or even months, in casual conversation with their targets before introducing the scam.

Many times, Scammers engage with their targets through fake social media profiles with attractive personas. They may flaunt a lavish lifestyle to appear successful, which often leads to conversations about investing and crypto, at which point they will introduce the scam.

Scammers won't directly ask for money from their targets. Instead, they will introduce the scam through some sort of unique crypto trading platform that promises huge returns in short periods of time. **In reality, these platforms are fraudulent; no real trading occurs and the Scammers have complete control over the platforms.**

Once a target is convinced to invest, the Scammer will then guide their target to convert their cash into crypto through a publicly known crypto exchange, crypto ATM, or digital wallet service, and then transfer crypto over to the fraudulent platform. **Please note that these crypto services are generally not in on the scam**; these are just channels used by Scammers to carry out their schemes.

"just fake numbers on a screen..."
These fraudulent platforms are designed to mirror the look and functionality of a real trading platform (e.g. real-time price charts, help desks, etc.) and may be available as mobile apps on the Apple App Store/Google Play. However, everything on the platform is fabricated (especially your account balance). These platforms are designed to keep targets engaged on the platform while finding other targets to scam until it is time to make off with stolen funds and shut down the platform.



6:50 5G

Wealth BAX

SAFE AND RELIABLE
24 HOURS CUSTOMER SERVICE ONLINE

Hots

BTC/USD		ETH/USD		LTC/USD	
Sell	Buy	Sell	Buy	Sell	Buy
59164.00	59164.01	2580.59	2580.60	64.05	64.06

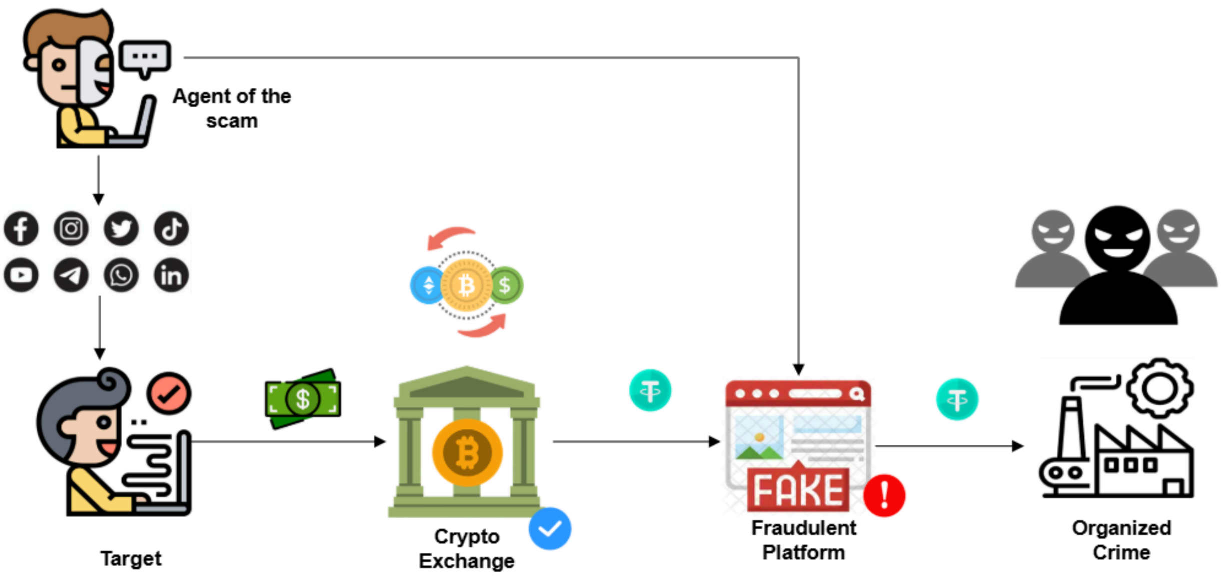
Contract Option

BTC/USD 21:50:51	59164.00 58548.23	59164.01 61400.00	-2.20
ETH/USD 21:50:50	2580.59 2555.00	2580.60 2695.00	-2.69
LTC/USD	64.05	64.06	-4.33

Home Position History User

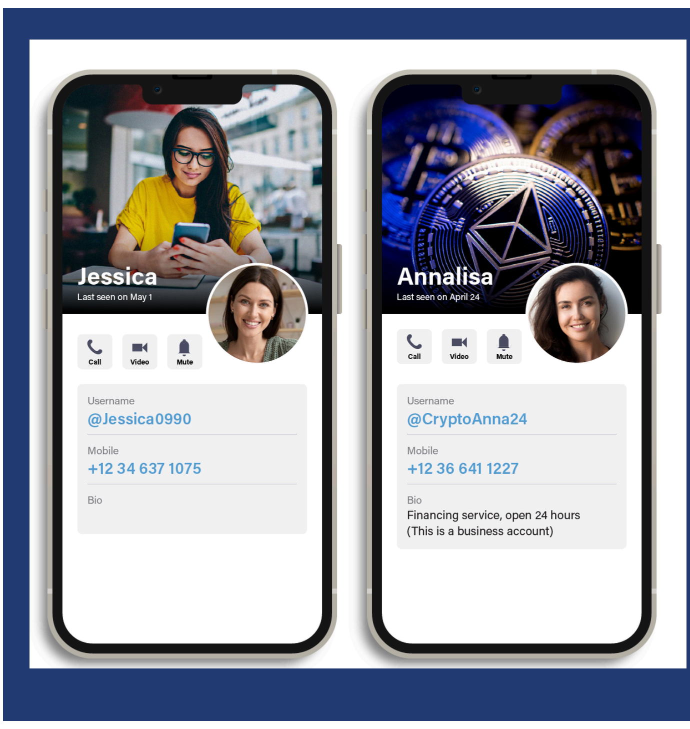
AA h5.wealthbax.com

Put this all together and this is what a pig butchering scam operation looks like behind the scenes:



Reporting on Crypto Scams

So what can I do if I encounter a crypto scam like a pig butchering scam?
The key thing is to report the scam to any financial regulator or law enforcement agency **as soon as possible**. The window of these scam operations are very small, so not only is it important to report an incident quickly, but it is also important to provide **the right details at the start**. Below are some tips for what information to provide when reporting a crypto scam to any regulatory or law enforcement agency:



Jessica
Last seen on May 1
Call Video Mute
Username
@Jessica0990
Mobile
+12 34 637 1075
Bio

Annalisa
Last seen on April 24
Call Video Mute
Username
@CryptoAnna24
Mobile
+12 36 641 1227
Bio
Financing service, open 24 hours
(This is a business account)

Identifying information about the Scammer(s)

Yes, the profiles of the scammers you are corresponding with are oftentimes fake. However, any information the scammer is presenting online can be useful in an investigation. Here are some examples of online information about the Scammer(s) you can include:

- Phone numbers, usernames, email addresses, and social media handles of scammer(s) you interacted with
- Screenshots of scammer's social media profile

Website(s) associated with the fraudulent platform

For us to investigate a fraudulent platform, it is important to provide all the website(s) associated with the fraud so we can investigate and shut them down. When :

- Include all website addresses you interacted with that are associated with the scam in your narrative of events
- Screenshots from your browser or screen grabs/recordings from your phone of the fraudulent platform with the website clearly visible if possible

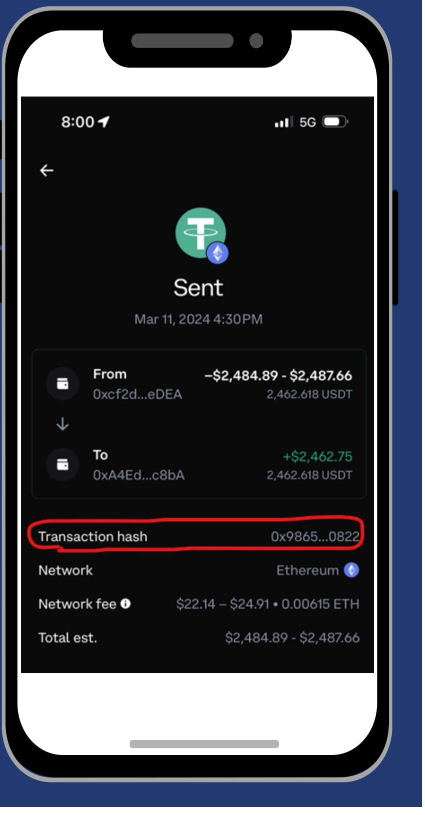
Financial transactions sent to the scammer

In order to find and trace the whereabouts of your particular stolen assets in a scam , there are key details we need to know about the transactions that took place. If you made transactions to the scammer using cryptocurrency, please indicate the following for **every** transaction you sent to the scammer:

- **Date** transaction(s) took place
- **Amount(s) sent** and **type of digital asset** (e.g. 0.5 ETH)
- **Wallet address** associated with the scammer
- **Transaction hash/ID** associated with the transaction
  - The transaction ID/hash is like a receipt for a crypto transaction

Ex. "12/22/24 - Sent 0.5 ETH to 0x..."
"On Dec 22, 2024 I sent 0.5 ETH to 0x..."
"Sent 0.5 ETH, tx hash: 0x230q24f...23"

Note: To find and trace your crypto on the blockchain, we need **complete and accurate** wallet addresses/transaction hashes. To avoid errors, we recommend copy and pasting this information in your complaint rather than typing it out manually.



8:00 5G
Sent
Mar 11, 2024 4:30PM

From 0xcf2d...eDEA	−$2,484.89 - $2,487.66 2,462.618 USDT
To 0xA4Ed...c8bA	+$2,462.75 2,462.618 USDT
Transaction hash	0x9865...0822
Network	Ethereum
Network fee	$22.14 – $24.91 • 0.00615 ETH
Total est.	$2,484.89 - $2,487.66

Our mission is to serve Californians by effectively overseeing financial service providers; enforcing laws and regulations; promoting innovation and fair and honest business practices; enhancing consumer awareness; and protecting consumers by preventing potential marketplace risks, fraud, and abuse. To better protect consumers from fraud and abuse in the crypto space, we need your help to provide us the information necessary to more effectively assess and investigate crypto scams.

Click here to submit a complaint to DFPI:
https://dfpi.ca.gov/submit-a-complaint/