Vol. 46, No. 2 • Fentanyl Advisements • Elder Neglect • Dark Web • Search Warrants • Opening and Closing • Pig Butchering Scam • Racial Justice Act

PROSECUTOR'S BRIEF

Vol. 46, No. 2 • Winter 2024

CDAA
California District Attorneys Association

Unveiling the Dark Side of Romance: *The Pig Butchering Scam*

by Erin West

Have you ever received an unexpected "wrong number" text message? Maybe it appears to be for someone else—perhaps a request for a veterinary appointment for a sick animal or a confirmation of a golf tee time? Have you noticed an increase in connection requests on your LinkedIn account or friend requests for Facebook, often by young, attractive Asian women who want to talk to you about investments in cryptocurrency?

If your answer is yes, you are experiencing step one of an elaborate romance and investment scam known as "Pig Butchering," which is financially devastating and emotionally crushing.

Meet Katie

Katie (not her real name) is a 32-year-old single woman in California who was looking for love on a dating app. After matching with an attractive international businessman, Ethan (not his real name) who allegedly lived in California, the two began chatting on the app until Ethan suggested they move their chat to WhatsApp. Within days, their chats became more frequent, and Katie found

Erin West is a Santa Clara County deputy district attorney with the REACT Task Force.

herself spending hours communicating with Ethan by text. Though his reluctance to speak on the phone seemed unusual to Katie, she accepted the explanations he gave. Meanwhile, the relationship began to deepen and soon he was calling her "honey" and talking about future travel plans together to exotic locations.

Ethan displayed an enviable lifestyle. He told Katie that he was headed out to shop for a new Rolex and shared pictures of meals from Michelin-starred restaurants. When Ethan told Katie that he made his money by investing in cryptocurrency, it fit. When he told her that he could help her do the same, she resisted, telling him she did not know much about it, and from what she did know, it was a good way to lose money.

Conversations became more intimate, and Ethan asked her to share her life struggles. Katie disclosed private information she held dear to her heart, and Ethan responded with considerate thoughts, creating a trust that would later come back to haunt her. Over time, Ethan learned how to provide the type of relationship Katie craved, sharing constant positivity and romantic wishes for the future.

Ethan preyed upon Katie's euphoria. Once he knew that he had her emotionally in pocket, he once again suggested investment in cryptocurrency, telling her that he would be with her every step of the way and would not let her lose a single dollar. So in she went, and with his guidance, invested $1,000 into a known commercial cryptocurrency platform and exchanged that $1,000 into a currency known as USDT or Tether. Ethan virtually held her hand as he directed her into putting her crypto into a fictitious trading platform, showing a dashboard that showed exponential gains.

Buoyed by the (fake) increase in her portfolio, Katie succumbed to Ethan's suggestions that she invest more. Ethan created false urgency and Katie responded, investing higher dollar amounts after being told her returns would increase. Meanwhile, Ethan turned up the volume on their relationship, sending romantic photos and saying suggestive things.

Katie began to imagine a time when she could pay off her used car and student loans. She was madly in love with a man who she thought shared her feelings. Emotions multiplied, and Katie found herself in the relationship of her dreams and a path to financial success.

When Katie tried to withdraw money from the account, she was advised that in order to do so, she would have to pay a 24 percent

tax on the value of the portfolio, and that money had to be new money. After much agitation, stress, and frustration, Katie was able to make that payment by taking out online loans and borrowing from relatives. But even after meeting this request, Katie was unable to access her money. Yet another roadblock stood in her way, in the form of a "security verification fee." To access her money, she would need to pay another fee. Again, she borrowed from relatives, but now also asked friends. Ethan assured her once this step was completed, she would have her funds in hand.

Of course, it did not work that way and there were other hoops to jump through to access her money. Katie was out of resources and patience. Finally, she confessed to her family the details of her investments, and it became crystal clear to all that Katie had been the target of a master manipulation plot and was out over $130,000. She sunk to the floor and cried as if there had been a death.

Pig Butchering Originated in China

The scam itself originated in China and was given the Chinese name Sha Zhu Pan, which translates in English to "pig butchering."[1] It is an elaborate form of romance fraud that involves scammers cultivating fake online romantic relationships with the intention of financially exploiting their victims. The name "pig butchering" comes from the act of systematically draining the victim's financial resources, akin to the dissection of a pig during the butchering process. Ultimately, the scammers look to consume the victim from snout to tail, taking every last cent from the victim. The scam typically unfolds in several stages, preying on victims' emotions and vulnerabilities.

The Stages

Katie's experience is typical of the pig butchering cases that law enforcement is seeing worldwide. Nearly every victim who comes forward will tell a similar story. Scammers have found that this technique works, so they reproduced it on a large scale.

Building Trust

Scammers initiate contact with unsuspecting individuals on dating websites, social media platforms, and/or email. They often use stolen photographs and fake profiles to create an attractive persona. Through regular communication and shared interests, they

build trust with their victims. This trust building stage is crucial, because ultimately, these scammers will ask their victims to do something they would not ordinarily do: Drain their savings and put the funds into cryptocurrency. Motivating that type of unusual behavior requires months of work at the outset to develop a level of confidence in the scammer that outweighs the risk.

During this initial period, scammers take great care to learn all they can about the victim's financial situation. Their aim is to take every penny from the victim, so it is important to explore all sources of income, e.g., a second home, wealthy parents, even friends.

Crafting a Story

Romance scammers weave intricate stories, often involving personal hardships or crises such as medical emergencies, legal troubles, or financial distress. These tales are designed to elicit sympathy and financial assistance from the victim. Scammers operate from a playbook, with chapters focused on each level of potential victim: a 30-year-old male software engineer, a 50-year-old divorced mom, or a 70-year-old man who has lost his wife.

Scammers spend time learning about their specific victim and mirroring back similar characteristics. If the victim has aging parents, so does the scammer. If a victim fears how he will pay for college for his kids, so does the scammer. Victims respond to this tactic because it feels familiar. Their new love is experiencing the same issues they are facing. It brings them closer and makes the relationship appear more genuine.

Investing

As the relationship deepens, scammers introduce the concept of shared investments or business opportunities. They persuade the victim to invest significant sums of money in these ventures, claiming substantial returns. Victims are lured into believing they are building a future together.

These victims will lack experience and familiarity with cryptocurrency, and that is where the trust factors in. The scammer will hold the victim's hand and guide them through every step of the process, often promising the victim that they will not lose any money. To overcome any reluctance, the scammer will suggest what they know to be a reasonably small amount for the first investment, perhaps $1,000 or $10,000, depending on the victim.

Technically speaking, the scammer will then assist the victim in moving funds from their existing accounts into a cryptocurrency exchange that the victim may have heard of, such as Coinbase or Crypto.com. The victim will set up a legitimate new account. From there, the scammer will assist the victim, often step by step with screenshots, with how to exchange those U.S. dollars into a coin called USDT or Tether. This coin is pegged to the U.S. dollar, which the victim can understand. Their $1,000 in U.S. dollars will be changed into about 1,000 Tether, less fees. This part is not challenging for victims to understand.

The next step is where the theft actually occurs. These scammers are masterful and have created web platforms that look exactly like existing investment sites. They are expertly crafted and by look and feel operate just like a true investment site. The scammer will then direct the victim to move the Tether out of the secure exchange account and into this platform.

What the victim will see is a beautiful dashboard showing a newly created account in their name. They will see their Tether in that account. As each day passes, they will see exponential growth in the account, leading them to believe that their money is dramatically increasing in value. The rise in value will be massive, and before they know it, their small initial investment will have doubled.

But that money is long gone. What the scammer has done behind the scenes is move that money straight into an account held by the scammer. The victim sees a fictitious accounting when accessing their account, because there is no account holding their currency. It has been passed on to account after account, designed to obfuscate the transfer, until it ultimately lands in the hands of Chinese organized crime.

Endorphins from the romantic relationship combined with the apparent evidence of wealth elevate the game. Shown incredible returns, victims are motivated and coerced into liquidating their retirement accounts, their kids' college accounts, and even taking lines of credit out against their homes.

Isolating the Victim

Scammers manipulate their victims emotionally and isolate them from friends and family, making it more challenging for the victim to seek advice or assistance. This isolation further entrenches

the victim in the scam. Scammers are well aware of the obstacles that will be put in place of the victim when they face their financial institutions, looking to withdraw massive amounts of money. Individuals who have been saving methodically for years will have to provide some sort of explanation to their bankers, and scammers prepare them for just that. Scammers will provide stories to the victims that they can use to justify these withdrawals, often that they are purchasing or remodeling real estate.

Paying Taxes

Once the scammer has seemingly drained the victim's financial resources, they wait. As they always do, the victim will attempt to take some of the money out of the account. That is when they are hit with a whammy and are told they have to pay taxes on the money, often in the neighborhood of 20 percent or more. When the victim attempts to pay those taxes out of the gains, they are told that it must be new money. Victims will then mortgage houses and beg family and friends to assist, thinking it will be a quick turnaround until they get access to their massive account.

Once those taxes are paid, there will be a new obstacle, such as an "identity verification" that will cost another $20,000 or a "withdrawal fee" of equally high expense. Depending on the victim, they will continue to scrape and scrounge to make that payment, or they will finally understand that this entire affair had been a scam from the beginning.

Ending the Charade

It is at this point that the victim will understand that the financial portion of the relationship was a scam. But they do not always realize that the relationship was a scam as well. Sometimes they try to band together with their scammer to go after the platform. These victims have been psychologically manipulated and it can be difficult to get them to see the full picture. This pattern then is repeated over and over with more victims.

Southeast Asia Is the Hotbed

This scam has victims on both sides of the operation. The Office of the United Nations High Commissioner for Human Rights (OHCHR) prepared a detailed report outlining the human trafficking conducted in Southeast Asia that provides the workforce

for the scam operation.[2] To staff this labor-intensive crime, crooks put their talent into creating fake trading platforms posing as beautiful websites soliciting talent. They advertise jobs in marketing, graphic design, sales, and call center work. These ads promise room and board, generous pay, and an attractive, comfortable place to work.

The reality is quite different. Once these employees arrive from their countries of origin, they are met at the airport. Their passports are taken, and they are bussed to places like vacated casinos of Sihanoukville, Cambodia, or compounds in Myanmar along the Thai border.[3] They are placed in locked facilities with bars on the windows and barbed wire along the walls. Guards with AK-47s stand by to make sure that no one escapes.[4] The United Nations estimates nearly 100,000 people are put into slavery in Cambodia and even more in Myanmar doing this work.[5]

Our world is overwhelmed with human trafficking victims scamming victims. The only winners are the syndicates running the entire operation.

Billions Are Lost

The syndicates behind these scams have stolen billions of dollars. Though they take time to develop, pig butchering scams are amazingly lucrative. Reports of losses in the millions of dollars to individual victims are not uncommon. Compounded from facility to facility, it is not difficult to imagine the dramatic transfer of wealth.

Last year, the FBI provided data detailing reports of $3.3 billion in crypto investment scams or pig butchering.[6] This data relies on the optional reporting by victims who are willing to type their information into the FBI's online reporting portal, known as IC3. But this crime carries shame and humiliation. While an individual might be willing to report a stolen car or home burglary, they are less willing to officially report that they were in an online relationship that they believed would lead to marriage and then transferred their entire net worth to an online platform they believed was tripling their money. Therein lies the problem. We know it is at least $3.3 billion, but likely 10 or more times that amount.

We are seeing an unprecedented movement of money. Household by household, we are moving a generation's worth of wealth into the hands of the unsavory. And, by all accounts, there is no end in sight.

Santa Clara County Takes Action

In March 2022, when the first reports of this type of crime began appearing in Santa Clara County, they appeared to be a difficult lift: suspects abroad, money going overseas. But District Attorney Jeff Rosen's high-tech task force, REACT, took up to the challenge.

When DA Rosen took office in 2011, he set forth a clear directive: He expected his office's high-tech task force to be the world leader for investigating and prosecuting high-tech crimes. REACT is a multijurisdictional task force made up of local detectives from agencies within its area of responsibility, which includes San Francisco, Alameda, San Mateo, Santa Clara, and Santa Cruz counties. It is an area of nearly six million people.

DA Rosen had foresight. Tech cases were going to become more frequent and digital evidence would permeate all of our cases, so a REACT agent was embedded with the FBI to learn investigative techniques. DA Rosen supports the training of all REACT agents at the nation's finest computer forensics institute, run by the United States Secret Service in Hoover, AL. He also supports innovation in this new area of technology.

When the first case of "SIM-swapping"[7] was reported in Santa Clara County in 2018, REACT agents doggedly researched this new crime. SIM-swapping involves hackers convincing employees at phone companies to redirect traffic from the target phone to a phone in possession of the hackers. This enabled hackers to defeat two-factor authentications by going to accounts owned by the target, clicking "forgot password" and having the code sent to the device that was now in possession of the hackers. By using this technique, hackers were able to take over email, social media, and cryptocurrency accounts of their victims. Millions of dollars were lost overnight and transferred into the hands of these criminals.

REACT solved this initial case and many more and was instrumental in arrests all over the world. REACT investigations led to the first prosecution and 10-year jail sentence of a SIM-swapper and then to a handful more. REACT had cemented its role as a world leader in high tech investigation and prosecution.

More importantly to the issue of pig butchering, REACT learned about cryptocurrency. Agents learned how to trace it on the blockchain; how to determine how and where it was held; how to draft and execute seizure orders; how to technically move the

cryptocurrency from the hands of the crooks to the hands of the government; and how to get it back in the hands of victims.

When it became clear that arrests of these pig butcherers were not in the cards, REACT followed the money. In May 2022, REACT embarked upon its first test case. A man known as Andrew (not his real name) is 30-year-old software engineer in San Jose. Andrew had been pig butchered and lost $300,000. REACT used commercially available software to trace the cryptocurrency and locate it at an exchange. The problem: There was no jurisdiction over the overseas exchange.

REACT reached out to the cryptocurrency exchange Binance who held the stolen funds. Binance agreed to return the funds upon receipt of a valid California search warrant. The warrant was drafted, signed, and produced, and Binance moved the money into REACT's government account. By late December 2022, Andrew and seven other victims received some of their money back. To date, REACT has been able to rinse and repeat this formula, helping 26 victims recover nearly $2.5 million.

As word got out of REACT's success, victims came in droves. REACT soon found that other agencies lacked the tools and education to investigate these crimes. In October 2022, the Crypto Coalition was formed, which joined 85 active law enforcement officials to hear a webinar from REACT about crypto investigations. Today, this group numbers more than 1,300 members from local, state, federal, and international law enforcement agencies and operates a highly active list serv. In January 2023, Santa Clara County hosted the first California Crypto Conference, offering hands-on, practical training in crypto investigation, taught by REACT and our partners at the United States Secret Service.

You Can Protect Yourself

Use the these tips to avoid being a victim of a pig butchering scam:

1. **Verify Identities**: Be wary of anyone who reaches out to you digitally. If you do not know the person, take a breath before you agree to connect. Verify their identity. Use reverse image searches to check if the photos they provide are genuine.
2. **Avoid Sharing Financial Information**: Never share your financial details or send money to someone you have met online, regardless of their emotional appeal.

3. **Be Cautious of Red Flags**: Pay attention to inconsistencies in their stories, reluctance to meet in person, and an excessive emphasis on financial matters. Scammers have playbooks about how to avoid video calls and what to say when the victim wants to meet them in person. Make sure those stories make sense.
4. **Maintain Privacy**: Be cautious about sharing personal information online and ensure your online profiles are set to private.
5. **Seek Advice**: If you suspect a scam, discuss it with friends or family, who can provide a different perspective and support. It can be uncomfortable to discuss these cases with others, but if something feels wrong, run it by someone else.
6. **Report Scammers**: If you encounter a romance scammer, report the incident immediately. Report your case to the local authorities, which will give them insight into how big the problem is in their community. File an online report at ic3.gov so that the FBI is notified and can aggregate data on a national level. Report the photo and name to the platform you met them on.

Pig butchering scams are cruel and heartless exploitations of individuals seeking love and companionship. Awareness and vigilance are our best weapons against these romance investment cons. By staying informed and being cautious when forming online relationships, we can protect ourselves and those we care about from falling victim to these manipulative and fraudulent practices. This crime will not stop until everyone knows about it. ■

ENDNOTES

1. Cezary Podkul, "What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One." (Sep. 19, 2022) *ProPublica* <*https://bit.ly/3uUwfJ4*> (accessed Dec. 12, 2023).
2. United Nations Human Rights Office of the High Commissioner, *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response* (2023) <*https://bit.ly/47T8fVd*> (accessed Dec. 12, 2023).
3. *Id*.
4. *Id*.
5. *Id*.
6. Federal Bureau of Investigation, Internet Crime Report 2022 <*https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf*> (accessed Jan. 9, 2024).
7. <*https://bit.ly/3GFuGBA*> (accessed Dec. 12, 2023).