HOMELAND SECURITY INVESTIGATIONS

CORNER$TONE

HSI FINANCIAL INVESTIGATIONS OUTREACH INITIATIVE

ISSUE #40
APR 2023

SPECIAL EDITION

HSI AND ACAMS ALERT: "PIG BUTCHERING"

HSI and ACAMS work closely to partner on a range of emerging financial crime typologies. Sharing information between the public and private sectors is one means to identify, report and mitigate such threats. This is why HSI and ACAMS have partnered through the Cornerstone initiative to reach the greatest number of anti-money laundering (AML) and compliance professionals possible about the devastating effects of pig butchering fraud. Fraud is a high priority concern for regulators, law enforcement and the general public alike. Over recent months, pig butchering — which encompasses multiple harms including large scale fraud, international money laundering, cyber-crime, people trafficking and modern slavery — has proliferated with terrible consequences for victims across the globe.

THE RISE OF PIG BUTCHERING GLOBALLY

Shāz Hū Pán otherwise known as pig butchering is an increasingly prolific financial fraud scheme, which combines elements of traditional romance and investment fraud whilst also targeting people trafficking and modern slavery victims. The typology generally (although not exclusively) is controlled by organized criminal gangs operating from Southeast Asia, including Special Economic Zones (SEZ) in countries like Myanmar, Laos, Cambodia and Thailand. In 2022, U.S. based victims alone lost approximately $3.3 billion dollars to crypto-related investment frauds.

Pig Butchering works by criminal networks placing fake job advertisements to attract young people from China and other countries. These individuals are then held, against their will, in secure compounds where they are forced (under threat of violence) to commit cyber enabled fraud against victims largely located in Western countries including the U.S. and Europe.

PIG BUTCHERING TACTICS

The following is a list of tactics, drawn from law enforcement investigations, employed by organized crime gangs to target their fraud victims:

- Pig butchering perpetrators operate as an organized structure of phone scammers, website designers and money mules.
- Targeted social engineering is used to engage victims and build trust.
- Perpetrators develop meaningful relationships with victims over months and engage

BE ON THE LOOKOUT FOR ISSUE #41 | MAY 2023
NEWLY IDENTIFIED TYPOLOGIES AND INDICATORS OF FRAUD

200+

DESIGNATED HSI CORNERSTONE REPRESENTATIVES ACROSS ALL HSI FIELD OFFICES

DID YOU KNOW?

HSI SPECIAL AGENTS ARE AVAILABLE TO PROVIDE TRAINING AND SHARE RED FLAG INDICATORS, CRIMINAL TYPOLOGIES, AND METHODS WITH BUSINESSES AND INDUSTRIES THAT MANAGE THE VERY SYSTEMS THAT TERRORISTS AND CRIMINAL ORGANIZATIONS SEEK TO EXPLOIT

CONTACT CORNERSTONE@HSI.DHS.GOV TO REQUEST A CORNERSTONE PRESENTATION

with victims on dating applications, social media platforms and voice-over-Internet protocol (VOIP) chat applications (e.g., Facebook Messenger, WhatsApp or Apple's iMessage).

- Geolocation services may also be exploited to make it appear that the scammer(s) is in the same location that the victim claims to be located in.
- Introducing high-yield investment opportunities in virtual assets such as cryptocurrency, foreign exchange or other commodities.
- Victims are often directed to open accounts through online investment websites (via Android or iOS) or virtual asset service providers (VASPs), such as cryptocurrency exchanges.
- Perpetrators often control the websites, using software that mimics investment portfolios or well-known cryptoasset exchanges, appearing to show high investment gains. Victims are provided with instructions to deposit money via wire transfer to shell companies, or via direct cryptocurrency transfer.
- The scammers pressure victims to invest more money and tie it to their personal relationship. When the victim tries to withdraw funds or shows signs of ending their investments, the account is closed and the money is gone. Some victims are asked to pay extra fees to withdraw money, while others are simply ignored and locked out of their accounts.

FINANCIAL INSTITUTIONS AND VASPS ARE EXPLOITED BY CRIMINALS

- Financial institutions and VASPs are unwittingly used as a conduit to collect and transfer deposits from victims and are primarily used as the first intermediaries to launder money overseas. Criminals exploit global financial chains to launder funds through correspondent banking relationships and additionally via the blockchain technology which underpins cryptoassets.
- Financial institutions are used to "on-ramp" and "off-ramp" virtual assets, like Ether and Tether, to and from a blockchain. Pig butchering schemes commonly involve victims withdrawing cash or initiating wire transfers to VASPs via their bank accounts.
- "Off-ramping" or cashing out their illicit financial proceeds can be done by using shell companies or crypto ATMs, or it can be done from cryptoasset exchanges registered in other countries, in jurisdictions with weak AML/CFT controls.
- Where VASPs are exploited, funds are quickly transferred into criminally controlled wallets. Criminal organizations employ money mules that open shell companies in the U.S., U.K. and elsewhere and create associated bank accounts and virtual asset wallets where victims send funds to the fraudulent investment scheme.

RED FLAG INDICATORS FOR TRADITIONAL FINANCIAL INSTITUTIONS

⌦ Individuals typically under the age of 40 years old with connections to the above-referenced countries, with no financial or investment background, open a business account on behalf of a newly created investment business.

⌦ Round dollar deposits over $1,000 from individuals geographically dispersed throughout the country, with no corresponding businesses services. Deposits from individuals increase over short periods of time to tens of thousands of dollars.

⌦ Same-day outbound transfers corresponding to the money from potential victims to keep daily balance at near

zero.

- Victims move money in round figures out of their account(s) e.g., $1,000 or $5,000.
- Trafficked persons may empty and close their accounts prior to moving overseas.

RED FLAG INDICATORS FOR VASPS

- Individual transfers virtual currency to one wallet address, and it is immediately moved to a common wallet, often holding $10-20 million on average.
- A new customer with no prior experience in virtual currencies begins sending numerous transfers in large amounts to the same wallet and does not send other transfers.
- Cash-to-crypto services are exchanging from one wallet address to fiat with no known link.
- Perpetrators use common laundering methods, like mixing services and chain hopping, to attempt to disguise the flow of funds.
- Funds that are routed through contract or liquidity mining schemes (fake decentralized schemes).
- Victims creating new accounts and initiating stable coin transactions, like U.S. Dollar Coin (USDC) or Tether (USDT), with no prior history of virtual asset trading.
- Wallets receiving transfers from victims initiating same-day outbound transfers to keep daily balance at near zero.
- Transactions that are funneled through decentralized exchanges to obfuscate the money trail.
- Funds being off ramped via different means, including transfers to non-compliant VASPs, cryptoasset gambling sites and potentially, over-the-counter crypto traders.

CUSTOMER DUE DILIGENCE (CDD) AND SUSPICIOUS ACTIVITY REPORTING

The Financial Action Task Force (FATF) recommendations outline a comprehensive and consistent framework of measures to combat financial crime. Furthermore, financial institutions can deploy a range of financial crime controls and mitigations as relevant to their country of registration.

FATF Recommendation 5 stipulates that financial institutions should be required to undertake customer due diligence (CDD) measures to guard against keeping anonymous accounts or accounts in fictitious names. CDD measures can include identifying customer and/or beneficial owner identity and conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship.

Financial Action Taskforce Recommendation 20 requires that, "if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity…it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)." Such reports are commonly known as Suspicious Transaction Reports (STRs) or Suspicious Activity Reports (SARs).

Examples of generic controls and mitigating activities to identify pig butchering may include:

- Enhanced scrutiny on "Know Your Customer" (KYC) requirements for new clients creating accounts for investment businesses.

- Applying enhanced due diligence (EDD) to business relationships and transactions with natural/legal persons to higher-risk transactions conducted through high-risk jurisdictions.
- Establishing jurisdictional policies, to prevent further movement of victim funds, that enable accounts to be frozen while checks on potentially fraudulent activity is undertaken.
- Establishing jurisdiction appropriate procedures for follow up with account owners of suspected fraud. This may include requesting supporting documentation such as invoices, evidence of investment, or wallet addresses money was transferred to.
- Contacting recipients of outbound transactions to raise awareness of scams and seek clarity to ensure transfers are for legitimate purposes.
- Implementing behavioral analysis techniques to detect and report deviation from normal customer behavior to mitigate risk and protect customers from becoming victims of fraud.
- Making use of blockchain analytics, machine learning tools and alert-generating software.
- Implementing appropriate training for all relevant employees to increase awareness of suspicious activity related to pig butchering, including consulting available Cornerstone and ACAMS' products.

Examples of specific mitigation efforts used by financial institutions in the U.S. may include:

- Leverage 314(b) under the Bank Secrecy Act or relevant domestic information sharing provisions in where an account owner is suspected of engaging in pig butchering frauds.
- Use of EDD procedures to ensure businesses and individuals have legitimate websites and are registered with the appropriate state and federal compliance office as applicable: Securities and Exchange Commission (SEC), Commodities Futures Trading Commission (CFTC), Financial Industry Regulatory Authority (FINRA), etc.

CONCLUSION

To effectively tackle frauds, including pig butchering, financial institutions and VASPs alike should assess their potential exposure to this typology. Law enforcement agencies must collaborate globally on investigations and the public and private sector must continue to collaborate through information sharing mechanisms. ACAMS and HSI will continue to work together to understand and share information about the development of pig butchering typologies and other forms of transnational fraud and money laundering.

If you need to report a financial fraud incident to HSI, please send details to NLDCFinancialLeads@hsi.dhs.gov

Please visit our webpage at and sign up for the monthly Cornerstone newsletter through GovDelivery

Visit Cornerstone on LinkedIn

Don't forget to check out ACAMS Insights to stay up-to-date on the latest happening in the anti-financial crime sector and follow ACAMS on LinkedIn