Written Testimony

OF

Erin West
Deputy District Attorney
REACT Task Force
Santa Clara County District Attorney's Office

BEFORE

Subcommittee on National Security, Illicit Finance, and International Financial Institutions
Committee on Financial Services
United States House of Representatives

ON

"Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry"

September 18, 2024
Washington, DC

Thank you, Chairman Luetkemeyer, Ranking Member Beatty, and distinguished Members of this subcommittee for holding this hearing and inviting me to participate. It is a true honor to be here today.

My name is Erin West. I've been a prosecutor with the Santa Clara County, California, District Attorney's Office for 26 years. I work for District Attorney Jeff Rosen and with the REACT task force, a California state-funded task force of local detectives specializing in cybercrime.

It is a pleasure to appear beside my federal partners who have submitted such impressive written testimony. United States Secret Service Cyber Policy Director Noyes, in particular, has provided a beautifully executed, comprehensive look at pig butchering and I agree with his remarks. I'm proud to sit beside representatives from the United States Treasury Department, who just this week sanctioned a major Cambodian kingpin in the pig butchering business and who has ties to the highest levels of Cambodian government. I'm grateful for their actions.

But I want to bring you testimony from a different position – from a person who has fielded hundreds of victim complaints for more than two years, struggling to find the right words to explain to broken humans what has happened to them and to help them understand the challenges in investigating their cases and recovering their stolen funds.

It is from that seat that I speak today.

I come before you as a fellow American who is witnessing the single worst financial attack on individual people this country has ever experienced.

I come before you as a local prosecutor representing the thousands of men and women in local law enforcement who lack the training, tools and bandwidth to help those in their jurisdiction who call them seeking help.

I come before you as a human being who is emotionally depleted from hearing victim after victim tell the same story of loss and having to tell them -- there is nothing I can do to help you.

I come before you as a woman who has literally and figuratively lost her voice from asking more and more loudly for the last two years for a national strategy and whole-of-government collaboration including state and local law enforcement.

We have reached crisis level and we must act today.

Let me tell you how we got to this point.

AMERICANS ARE GETTING DESTROYED FINANCIALLY AND EMOTIONALLY

In March 2022, my task force saw our first pig butchering case. A 30-year-old software engineer I will call Evan seemingly had it all: a good job, cadre of friends, and a large chunk of money set aside for the future. Evan was ready for the next step. He wanted to find a life companion. Online he met a woman whom he thought could be just that. As they got to know each other through hours of texting daily, they became closer and closer. He was in love.

During their conversations, his new love would discuss high-end travel and expensive hobbies, displaying a lavish lifestyle. Ultimately, she disclosed that she achieved this through investing in cryptocurrency. She told Evan that she didn't know much about how to do it, but her uncle taught her, and her uncle would be happy to teach Evan.

There began the financial fraud. Overwhelmed with endorphins and all the good feelings that come with a new relationship, and backed up with his girlfriend's display of wealth, Evan was talked into investing in cryptocurrency.

Pig butchering is exponentially more destructive than any other romance scam we've ever seen, because it preys on the entire net worth of the victim. The scammer spends serious time learning the extent of the financial position of the victim, so the pressure continues until the victim has liquidated their 401k and depleted their children's college accounts. The term pig butchering is a translation of the Chinese phrase "sha zu pan," which is what the scammers call it. They will consume a victim from "snout to tail," leaving no meat on the bone. Pig butchering doesn't end until the scammer has taken every last penny from the victim.

Here's how a typical version of this scam works:

1. The victim is encouraged to transfer a small amount of money from his American bank to a known cryptocurrency exchange located in the United States. The victim opens the cryptocurrency account, provides the Know Your Customer information, and has full control of the exchange account.

2. Once the US dollars are in the crypto account, the scammer explains to the victim step-by-step how to convert them into a stablecoin known as USDT/Tether. The Tether remains in the wallet at the exchange under the victim's full control.

3. Now the theft occurs: The scammer lures the victim into moving the money from the exchange wallet into an "investment platform." Right now there are thousands and thousands of scam platforms just like this that are live on the internet, stealing American money as you read this document.

4. The victim is led to believe that he has now invested into an investment platform. He is shown an attractive dashboard displaying that the value of his investment has gone up exponentially, and before the end of the week it has doubled. In reality, the platform is fake, the dashboard is manufactured, and his money is in the hands of the scammers, moving through mule accounts down the blockchain.

5. Buoyed by the success, feeling like he's met the woman of his dreams and hit the investment jackpot, the victim is lured to liquidate his retirement accounts and invest everything he has. His phony investment portfolio nears a million dollars.

6. Seeing such a massive number on his dashboard, the victim is ready to enjoy some of these funds. When the victim attempts to withdraw money, he is hit with a tax bill. The scammers demand a phony tax of 25% of the account's value. When the victim suggests that the scammers take the money from the gains, he is told that it must be new funds. That's when our victims return to their banks to get lines of credit, or even worse, do a quick high-interest loan because they believe they will get access to their million-dollar accounts.

7. Some victims realize that they have been scammed when the taxes are demanded. However, others still make that payment and are hit with further requests for "identity verification" or some other disingenuous hurdle. Ultimately, they realize that the entire business was a scam, and worse yet, that the person they trust most in life was in on it from the beginning. The devastation is massive and sometimes deadly.

Returning to Evan's case, the REACT detectives traced and located a substantial portion of his money housed in an overseas crypto exchange. We innovated and shoehorned our practice into existing law, recovered a large part of those funds, and then returned them to him. We did it 25 more times before the criminals got smarter, the funds moved off exchanges faster, and the process no longer worked.

We also learned quickly that Evan was not alone. Our Santa Clara County victims had lost entire nest eggs. They were suicidal. One victim, the adult son and sole supporter of his immigrant parents, showed me a text conversation where he had told the scammer that if he were to lose his funds, he would "suicide in secret." Her response: "Trust me. Your money is safe." When this man came to realize that he had lost everything, he couldn't imagine a way forward and checked himself into a psychiatric hospital. Over two years later, he still suffers the mental anguish of this loss and is currently on disability leave from his job.

Yet another Santa Clara County victim attempted suicide. This man worked in the cybersecurity field and asked me to help train his trade organization about the dangers of pig butchering. Before I got even 10 minutes into my presentation, a man raised his hand and said "I just don't think I would ever fall for that." Maybe he wouldn't. But another man in his community did. And nearly died as a result.

Victim reports kept coming in. Finding ourselves lacking peers, we reached out nationwide to find other law enforcement doing this work. We were delighted to find expertise at the Manhattan and Queens' District Attorneys' Offices. We found dedicated skilled detectives with the Connecticut State Police and the small city of Brooklyn Park, MN. We pulled them all together, and in October 2022 we held a webinar to educate about pig butchering, and the Crypto Coalition was born. The 85 members who showed up for that webinar have now grown to more than 2,000 active members of law enforcement who specialize in cryptocurrency investigations.

Today, I represent not only my County, but also my state and local partners in the Crypto Coalition who don't have the opportunity to be here.

The Crypto Coalition listserv provides practical information sharing, our shared library teems with warrants and best practices, and our webinars draw hundreds as we keep ourselves educated and current in this rapidly changing ecosystem. We found that cooperation and collaboration were indispensable to navigating this new technology. Never before had local and state law enforcement had an opportunity to access their peers doing the same type of work. This Coalition has been a fundamental step forward in the ability of local and state governments to serve victims. But it isn't enough: the need for affordable tools and training continues to plague my peers.

The method we pioneered at the Santa Clara County DA's Office to trace, seize and return stolen crypto from this scam, we taught others to do, and Coalition members across the country have done it lots and lots and lots of times. And still we are returning just a tiny fraction of the money being stolen from our neighbors, relatives, and friends across America.

As the Coalition developed, I was pleased to see progress in how our local and state entities were able to serve victims, but the cases kept coming. In droves. More and more people were wholly decimated and unable to get assistance. More troubling stories emerged. An adult son told me that his Florida-based mother recently called him to say she didn't have money to pay her mortgage. "You don't have a mortgage," he told her. "Now I do," she said, ultimately disclosing that she had been trapped in a pig butchering scheme and that the scammer had shown her how to "invest" more by teaching her step-by-step how to take out an online mortgage against her home.

Other stories were even more grave. An adult daughter in Michigan confided that her father had killed himself. She had no idea why until she started to look through his digital life and found that immersed in a pig butchering scam, he lost the family fortune. He saw no alternative. I talked to an adult daughter in California whose father had killed himself. She didn't know why until she discovered that he was a victim of a $3 million loss in a pig butchering scam. Yet another family lost a father to suicide in Maryland. These reports continue to come in at uncomfortably regular intervals, not remotely slowing down. Hollywood even depicted it pretty accurately in the opening scenes of the recent blockbuster movie, "The Beekeeper."

These nationwide reports come directly to me because of the reputation we have built at REACT. They show an even more disturbing trend: our victims are unable to get any help from their local police, and they aren't hearing anything back from our federal government. By the time their emails reach my inbox, they are out of gas. Exhausted. Distraught. Unable to conceive that they had hundreds of thousands of dollars stolen from them and that nobody cares. Victims are becoming increasingly dissatisfied with the lack of assistance and soon find themselves googling solutions, landing them further in debt as they became secondarily scammed by "crypto recovery agents" charging thousands of dollars and falsely promising the ability to return funds.

The situation for victims worsens as the criminal enterprise pivots. Rather than allow funds to sit in an exchange account long enough for law enforcement to grab them, the scammers are moving money out at the speed of light. No matter how fast we are, the scammers are always faster. Our methodology for helping victims no longer works as well. Victims are increasing in numbers. More and more money is lost.

Coalition members have developed other blueprints for action as well. One of our best triumphs came from Alona Katz, Chief of the Virtual Currency Unit, Brooklyn District Attorney's Office. After watching Brooklyn victims lose money repeatedly to a scam operation targeting members of the Russian community, Alona taught herself how to analyze the domains and find other live domains sharing the same characteristics. She then seized 70 fraudulent domains, interrupting scams in progress and saving Brooklyners and others from further losses. When she and her District Attorney, Eric Gonzalez, publicly announced this win, they further took the opportunity to educate potential victims of online scams.

We've achieved successes, but in context of the grand scale of this transnational organized crime epidemic, they are not nearly enough and do not address directly enough the fight we are in.

The problem requires a national solution. We must act today.

CHINESE ORGANIZED CRIME SYNDICATES ARE BEHIND THE CRISIS

With victimization showing no signs of slowing, I began to look abroad to better understand the geopolitical issues enabling this crisis. As a member of the Senior Study Group assembled by the United States Institute of Peace (USIP), I traveled to Southeast Asia twice in the last year to provide insight for the paper released in May 2024: "Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security.[1]"

What I learned was disturbing: at the heart of this humanitarian disaster stands known Chinese organized crime syndicates. The organizations that have migrated to Southeast Asia over the last several decades now hold unprecedented power over the region. They have thoroughly embedded themselves in highly corrupt and unstable countries where they are not operating on the margins, but at the epicenter of the political and economic landscape. USIP and the UN Office of Drugs and Crime (UNODC) have estimated that revenue generated by this criminal industry comprises more than 40% of the combined GDP of Cambodia, Myanmar and Laos… the epicenter countries. In Cambodia particularly, this can be viewed as a state-run criminal enterprise with compounds owned by senators, governors, cabinet members, advisors to and family members of the Prime Minister. While pig butchering was primarily based in compounds, casino towers and office buildings in Southeast Asia, we are now seeing a global footprint spreading to the Middle East and Africa.

---

[1] https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security

Well-run syndicates are sophisticated, organized and operate at an industrial level. These scam centers are largely staffed by human-trafficked victims who have been led to believe they have been hired for a plush live/work office job. They have responded to online ads seeking workers, provided resumes and sat for interviews. They have every reason to believe that the offer of employment is genuine.

After taking company-funded flights to the region, they are met upon arrival and their passports are taken. They are bussed to compounds surrounded by barbed wire and guarded by men with AK-47s. Their actual employment is now revealed: they will be working 17 hours a day to scam Americans (and others worldwide) and to steal all of their money. Violence is common and is perpetrated in front of other employees. Those who do not meet quotas are beaten with baseball bats. They are hit with electric batons. Women who are not good at scamming are repurposed to provide sexual rewards for bosses and those who are hitting scam targets. Suicides from inside the compounds are common.

In Cambodia, towers filled with human trafficked victims are forced to conduct this dirty business, shielded from disruption by the rampant corruption that rises to the top of government. In Myanmar, as a civil war rages, dozens and dozens of compounds continue to grow along the Moei river. For more than four years now, these enclaves have been virtually untouched by enforcement, which has allowed them to grow, flourish and develop. They are massive cities of crime, solely dedicated to stealing wealth from the rest of the world.

We must act today.

TRANSNATIONAL ORGANIZED CRIME THREATENS NATIONAL SECURITY

Statistics from the FBI's IC3.gov victim-reporting portal show that investment fraud losses rose from $3.31 billion in 2022 to $4.57 billion in 2023, a 38% increase[2]. Confidence/romance scam reports numbered $652 million in 2023, bringing the combined total of victim losses to pig butchering to more than $5 billion last year. The actual amount of victim losses is exponentially higher than that. Frequently I talk to victims who are too embarrassed or humiliated to come forward. Losing money in a pig butchering scam carries a significant stigma that stifles reporting. If only half of victims report (and it's likely much less than that), we can estimate a problem of more than $10 billion last year in the United States. A conservative estimate of worldwide funds stolen in these schemes numbers $64 billion, according to the United States Institute of Peace.[3] Without accurate data, it is difficult to quantify the extent of the problem.

Though we may not know the exact number, what we do know is that billions of dollars are being transferred, household by household into the hands of known Chinese organized criminal syndicates. An incomprehensible amount of money is being stolen from our neighbors, our doctors, our teachers and even our financial advisors and is being moved out of the American financial system. Rather than transfer inheritance into the hands of their children, baby boomers are moving generational wealth into the hands of organized crime outside the United States. An

---

[2] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, p. 21.

[3] https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security, p. 8.

unprecedented movement of this level of wealth into the hands of bad actors must sound alarms in government.

Noting the rise and impact of transnational organized crime in Southeast Asia, the United States Institute of Peace convened a Senior Study Group. I am proud to have participated in this work. The 68-page document produced by the group in May 2024 details concerns: "Since 2021, the power, reach, and influence of these criminal networks have expanded to the point that they now directly threaten human security globally while posing a growing threat to the national security of the United States and many of its allies and partners around the world."

The USIP report emphasizes the gradual and notable rise in power of the syndicates: "Over the past decade Southeast Asia has become a major breeding ground for criminal networks emanating predominantly from China," and concern is well founded. "Ample evidence suggests that protection of the scamming industry is now of strategic interest to the ruling elites in Myanmar, Cambodia, and other countries in the region due to the industry's profitability and the nature of state involvement."[4]

WE MUST ORGANIZE AND FIGHT TOGETHER
--ENTER OPERATION SHAMROCK--

This disturbing status quo thrives on and will ultimately outwit a partial or disjointed international response. We lack a national strategy. We are siloed and overwhelmed with bureaucracy and red tape. We are missing opportunities to pair private industry solutions with government enforcement. As a nation, we have done very little to disrupt this criminal industry and to protect our citizens from the relentless threat that comes at them daily. As a result, those of us on the ground floor taking citizen complaints are seeing humans who are emotionally broken and are getting no help from either state, local or federal law enforcement.

We have been too slow to understand the gravity of the problem. As we dismiss this as "just fraud," a novel war has been declared against us. The enemy has weaponized the financial system, is using tried and true psychological tricks against our citizens and is systematically draining our coffers one household at a time. It must stop.

Certainly, there is no easy or single way to stop this crisis. A problem with so many dimensions requires partners from all sectors. It was with that mindset that I founded Operation Shamrock in April of this year with three thought leaders: Esteban Castaño, CEO of TRM Labs, a blockchain intelligence company that helps identify and disrupt illicit use of cryptocurrency; Matt O'Neill, who recently retired after 25 years with the United States Secret Service, most recently running the Global Investigative Operations Center; and Jacob Sims, a Southeast Asia regional expert who works with both International Justice Mission and United States Institute of Peace.

Operation Shamrock is the first and largest cross-industry, information-sharing coalition against transnational organized crime in Southeast Asia. We have assembled partners from all sectors of

[4] https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security, p. 8-9.

the pig butchering life cycle, including social media, banking and financial services, cryptocurrency exchanges, NGOs and victim services.

Beyond my partners in law enforcement, today through Operation Shamrock, I also represent an enormous group of civil society, the private sector, and stakeholders from around the world who are banding together to undermine the global pig butchering epidemic.

Shamrock is divided into five working groups: Tech, Law Enforcement, Banking/Financial Institutions, Foreign Policy and Victim Services. Each group has strong leadership and a set of milestone goals. We are six months in and our achievements are already moving the needle:

-Developed a smoother victim reporting system that accelerates the cases most likely to achieve a financial recovery to a team of vetted investigators for immediate tracing;

-Developed a standardized response letter for victims, expressing empathy, setting reasonable expectations for law enforcement and advising of available services;

-Trained hundreds of law enforcement partners through Crypto Coalition webinars hosting industry leaders from Binance, Coinbase, CashApp and OKX, among others, which foster a better inter-industry working community;

-Scheduled two weeks of law enforcement training webinars (starting 9/16/24) to provide basic and advanced education valuable to all levels of crypto investigation;

-Brought law enforcement and banking experts together to train hundreds of credit unions, small banks, and big banks about the pig butchering typology, what it will look like when it comes into the branch, and how to help a customer recognize the scam;

-Created resource guides for front-line banking employees about how to handle pig butchering cases;

-Created a slide deck about basic scams and pig butchering and trained hundreds of volunteers how to present those slides to community groups, workplaces and churches;

-Increased media coverage about pig butchering by working with the New York Times, the Wall Street Journal, CNN, ABC, CNBC, Late Night with John Oliver and 60 Minutes Australia to create pieces that will educate potential victims.

Operation Shamrock is one piece of the solution, but nothing will change until we have a coordinated American response to this international crisis.

TODAY'S CONGRESS MUST MANDATE IDENTIFICATION OF A SCAM CZAR

Bad actors continue to benefit from our inability to organize ourselves. For years Chinese organized crime syndicates have honed their collective craft of scamming the rest of the world. We cannot wait one day longer to identify a Scam Czar and create a national task force, made up

of all industries that touch any part of the pig butchering life cycle. This task force must be given adequate resources to accomplish objectives. We are at war, and we must fund a response.

The task force's first priority is to develop a national strategy which relies on a divide-and-conquer philosophy. Our government is made up of individual agencies, all with their own independent tools and mandates. It's time to acknowledge respective strengths and weaknesses and divide tasks accordingly. We build a team made up of multiple agencies, each using their biggest strengths. Subgroups of this team would focus on an effort to educate, seize and disrupt:

-education of the public about the nature of the scam
-education of law enforcement to respond to victims
-seizure
-enforcement
-sanctions
-taking down scam websites
-working with social media to rid platforms of bad actors
-slowing down bank transfers where a scam is suspected
-disrupting internet service to compounds

Sanctioning Ly Yung Phat and his businesses was a good start. We must identify and sanction more people overseas who are engaging in this scam and running it.

More than that we need to build criminal cases against them to extradite and prosecute them for these crimes.

We must stop burdening victims with reporting to 17 different agencies. Victims should report to one central location, and that portal should contain fields to ingest all relevant categories of data. Victims must be given acknowledgement of receipt of report and a reasonable set of expectations. From the singular reporting platform, we will be able to get a more accurate data set that captures total dollar amount of loss and attributes it to the correct typology.

We must fund our state and local law enforcement to help them learn how to and have the time to help the victims throughout our country in real time as the scams are occurring.

We must pass sensible laws that slow down fraud transactions to give the victim time to stop the scams, and to give law enforcement new tools to seize and return stolen funds.

Additional policy recommendations from Operation Shamrock are contained in the white paper titled "Tackling Pig Butchering" and attached hereto.

More than a year ago, I was asked to speak at an event hosted by the FBI and a social media company. As I laid out the scope of the problem, I specifically argued the need for a national leader. As 15 months have passed since, with still no national leadership, billions more have been transferred from American victims to Chinese organized crime. We need to act now.

The American response is disorganized. We are wasting resources replicating efforts. We don't have visibility to what other agencies are doing. We haven't identified common goals. It's literally killing our citizens and victims abroad. We aren't moving forward in a way that closes in our enemy. They continue to outpace us and move further and further ahead. We cannot let another day pass without a leader and a solution.

Thank you for the opportunity to appear before you to discuss a rapidly rising national security threat that we can no longer afford to ignore. I look forward to your questions.

Tackling Pig Butchering

A Strategic Framework for Tackling Pig Butchering and Other Online Fraud

Operation Shamrock White Paper
Version 0.1
April 5, 2024

Authors:
Erin West, Deputy District Attorney, Santa Clara County
Matthew O'Neill, Co-Founder/Partner at 5OH Consulting LLC
Esteban Castaño, CEO, TRM Labs
Jacob Sims, Global Advisor - Forced Criminality, International Justice Mission

Contents

Introduction

This draft white paper proposes a strategic framework to combat the global menace of pig butchering scams and other forms of online fraud, both current and those yet to emerge.

This initial draft draws on insights gleaned from discussions with over 30 subject-matter experts across various fields–including academia, law enforcement, regulatory agencies, crypto businesses, social media platforms, online dating platforms, telecommunications companies, financial institutions, international public sector entities, and nonprofits.

The solutions presented are by no means exhaustive and should not be seen as formal recommendations. Furthermore, they might not reflect the unanimous views of all authors involved. The purpose of this document is to gather a wide variety of perspectives, thereby stimulating debate on the efficacy and potential downsides of the proposed solutions. It is intended to act as a catalyst for further discussion and refinement, with subsequent versions focusing more closely on particular strategies and the progress made in implementing them.

Get involved

In the face of a global crisis, a global remedy is imperative. Until now, each of the affected sectors have approached the issue of pig butchering with narrow perspectives, focusing on their own limited aspects of the overarching crisis. Organizations maintain and do not share their data sets, limiting visibility by others. It is only by integrating all these fragments that we can effectively tackle this problem.

We are at a pivotal juncture where both the private and public sectors are willing to engage and collaborate. It is time to build on this momentum and cooperatively move forward against a common enemy.

Operation Shamrock is running a series of working groups over the course of 2024 to push forward the most promising solutions. **Join a team via this form.**

In addition, we invite you to **shape the next iteration of this white paper by sharing your ideas, queries, and concerns through this form or by leaving a comment directly on the online version of this white paper here.**

What is Pig Butchering?

"Pig Butchering" scams, also known as "sha zhu pan," involve a series of manipulative tactics aimed at defrauding victims through fake relationships and fraudulent investment opportunities. These scams typically unfold in several stages:

- **Initial Contact:** The scammer reaches out to potential victims through social media, dating apps, or even random text messages, often pretending to have contacted the wrong number. This strategy is to establish communication and begin building trust.
- **Building Trust**: Over time, scammers foster a relationship, sometimes romantic or platonic, by engaging in regular and personal conversations. This period of relationship-building is critical for the scam to succeed, as it establishes a bond and a level of trust between the scammer and the victim.
- **Introducing Investment:** After trust has been built, the scammer introduces the idea of a lucrative investment opportunity, typically involving cryptocurrencies. They may show evidence of their own success or offer to share insider knowledge to persuade the victim to invest.
- **Investment and Theft:** Victims are directed to fake investment websites or apps, where they can "manage" their investments. Scammers may even allow victims to withdraw a small amount initially to foster a false sense of security. Ultimately, victims are encouraged to invest increasingly larger sums until they are financially overextended.
- **Disappearance and Loss:** Once the victim is unable to invest more or decides to withdraw their funds, the scammers cut off communication and disappear. By this point, the victim's money has been transferred to the scammer, and recovery is often impossible due to the speed at which the scammer launders and cashes out of the stolen funds.

The impact of these scams is not only financial; victims often suffer significant emotional distress after realizing the personal connection they believed they had was a ruse.

Pig Butchering: A National Security Threat

Pig butchering scams, orchestrated by transnational organized crime groups (TOCs), are a growing national security threat. These scams inflict a devastating human cost, shattering lives and causing emotional turmoil alongside significant financial losses. While the direct human cost is devastating, the spillover effects are having a significant impact on global security.

Pig butchering scams, alongside other forms of investment fraud and romance scams, are believed to generate upwards of $12 billion for TOCs, fueling a dangerous financial ecosystem that threatens global security. The United Nations Office on Drugs and Crime (UNODC) has highlighted that, in just one Southeast Asian country, earnings from such scams are estimated to be in the range of $7.5 to $12.5 billion. TRM Labs, a blockchain intelligence firm specializing in tracking illicit cryptocurrency transactions, identified over $12.5 billion of cryptocurrency funneled into fraud schemes in 2023, with pig butchering scams accounting for at least $4.5 billion of this total. The FBI's Internet Crime Complaint Center (IC3) reports that losses to investment fraud became the most of any crime type tracked by IC3, witnessing a 38% increase from $3.31 billion in 2022 to $4.57 billion in 2023. In the United Kingdom, Action Fraud reported that citizens lost at least £2.35 billion to fraud in 2021. Furthermore, the 2022 Targeting Scams report indicated that Australians suffered over $3 billion in losses due to scams in 2022, marking an 80% surge from the previous year's totals. These figures likely represent just a fraction of the actual losses, as the shame and devastation experienced by victims often deter them from reporting these crimes and many countries' losses are not included.

Fraud profits fuel corruption and regional instability. Proceeds of fraud infiltrate economies, corrupt officials, and weaken legitimate governance. For instance, the UNODC estimates this crime could account for up to USD12.5 billion per year – half the annual GDP – in Cambodia alone. While pig butchering is just the most recent in a long history of Cambodia state-facilitated criminal industries, the scale and sophistication is unprecedented. In Cambodia, Myanmar, and Laos, police and court systems are often rendered impotent as scam operators either operate beyond the reach of the state or have purchased state protection. Many compounds themselves are owned by prominent members of the ruling elite, including, in some cases, family members and close business associates of heads of state. The sheer scale of the

industry is fundamentally redefining the political and economic landscape in Southeast Asia. The hyper lucrative nature of industrial-scale scamming encourages further criminal activity and weakens governments' ability to maintain stability.
TOCs are fueling the development of money laundering infrastructure. With cover from their co-conspirators in regional governments, TOCs are investing in casinos, e-junkets, and cryptocurrency exchanges, creating a sophisticated network to clean their ill-gotten gains. This industrial "money laundering as a service" infrastructure risks being exploited by a wide range of criminal actors, including state-facilitated hacking groups, drug cartels, and terrorist organizations. Casinos have long been used as a tool for money laundering; for instance, the Lazarus Group is believed to have laundered money stolen from the Bangladesh bank heist through casinos.

The human cost of pig butchering scams cannot be overstated. Victims are often subjected to psychological manipulation, leading to emotional distress and social isolation. The financial losses can be life-altering, jeopardizing victims' futures and leaving them struggling to meet basic needs. If and when victims report to law enforcement, many are turned away due to law enforcement bandwidth limitations or lack of familiarity with investigating these crimes. Moreover, many of the perpetrators of these scams are human trafficking victims themselves, lured by seemingly legitimate job opportunities, often kidnapped and forced to work in brutal conditions within heavily guarded compounds. While reports differ, the UN estimates that there may be as many as 220,000 labor trafficking victims at the bottom of this industry in Cambodia and Myanmar alone.

The future of fraud is catastrophic scale, powered by AI. TOCs are already investing in generative AI to expand their operations. Large language models (LLMs) like ChatGPT enable fraudsters to translate their scripts and playbooks, enabling them to target victims across more languages and countries. They also use LLMs to better simulate their persona and carry on more realistic conversations. “AI Agents”, or autonomous AI bots, will enable TOCs to hyper-scale their operations by lessening their reliance on humans behind the keyboard. TOCs will be able to spin up tens of thousands of AI agents trained to identify victims and execute scams. Imagine pig butchering scams targeting not just thousands, but millions of victims simultaneously, unencumbered by human resources. This chilling prospect is closer than we think.

The fight against pig butchering isn't just about protecting individual scam and human trafficking victims. It's about dismantling a financial engine funneling billions of dollars to global criminal networks.

Solution Landscape

The solutions detailed herein are not comprehensive, should not be interpreted as formal recommendations, and may not always represent the views of every author. The intent is to assemble a broad range of ideas, thereby facilitating discussions on the merits and drawbacks of various proposed solutions.

I. BLOCK FRAUD

Warn users “just-in-time” across the scam lifecycle

Description

Integrate tailored warnings and guidance for users at crucial moments in the scam lifecycle, starting from the initial contact by a scammer through a messaging app, to the point where a payment to the scammer is executed. This strategy ensures users are informed and cautious at each step where they're most vulnerable to fraud.

Obstacles

- **Companies might lack sufficient incentives** to implement user protections against scams and fraud without clear financial benefits or regulatory pressures, such as the UK's Contingent Reimbursement Model. Discussions with entities across social media, messaging, and dating platforms indicate that revenue drivers such as increased user retention, cost savings from reduced chargebacks, along with diminished reputational and regulatory risks, are key drivers for fraud prevention investments. Without these financial or regulatory incentives, businesses may not be motivated to further invest in safeguarding their users from fraud.
- **Issuing warnings at the payment stage may not effectively deter fraud victims**, who may have been preconditioned by scammers to disregard such alerts. A study highlighted by the UK House of Lords indicates that despite Revolut’s implementation of unavoidable Instagram-style stories to caution users about high-risk payments, a significant majority overlook these warnings. Even when Revolut's algorithms successfully flag potential Authorized Push Payment (APP) fraud, the majority of users proceed with their transactions, unaffected by direct warnings or even after discussing risks with a representative. This suggests that frequent, generic warnings may desensitize users, making them less likely to heed genuine alerts. Similarly, attempts by a leading cryptocurrency exchange to introduce scam warnings during withdrawal transactions were ineffective, as victims frequently overlooked these alerts, influenced by the scammer's persuasive trust-building. This scenario not only highlights the scammers' persuasive hold over victims but also underscores the crucial need for implementing such warnings earlier in the scam lifecycle.

Introducing warnings before the victim develops trust in the scammer — such as when the scammer initially contacts the victim via a social media or dating platform — could significantly enhance these warnings' effectiveness, providing a critical intervention point that could potentially halt the scam in its tracks.

Opportunities

- **Issuing warnings when scammers first initiate contact with victims:** Communication companies, including social media, messaging apps, telecom services, and dating platforms, could warn users about scams and frauds. Implementing real-time warnings within the chat interfaces can alert users about potential scams from the moment of initial contact by a scammer, akin to phishing alerts in email services. These warnings could be based on patterns such as messages from strangers or accounts with high messaging volumes. Insights from the integration of warnings within the payment process highlight that by the time a user reaches this stage, they have often already been persuaded by the scammer, rendering such warnings less effective. Therefore, it's crucial to intercept and warn users at earlier stages of potential fraud, specifically at the onset of communication with scammers. Early intervention through education and alerts within these communication platforms can play a pivotal role in preventing users from falling prey to scams, by disrupting the scam lifecycle before victims become too invested.
- **Issuing warnings before payment:** Financial institutions, including banks and virtual asset exchanges, can integrate tailored warnings about different types of fraud when they transfer money. For example, in 2019, Santander integrated tailored fraud warnings on their banking app. Individuals should be strongly encouraged to verify the identity of the receiving party - whether on their own or using solutions provided by their financial institution.
- **Alerting customers of scam signs after suspicious withdrawal**: Crypto exchanges could help victims reduce future losses by warning them after they make a first payment. For instance, if a withdrawal seems suspicious (e.g., a newly created account initiates a withdrawal of a round amount to a new address with no prior activity, or moving to an address that later consolidates funds with one linked to scams), the exchange could notify the user via both email and phone call. These notifications could highlight the withdrawal's suspicious nature and caution users against common indicators of pig butchering scams, such as unexpected online connections promoting cryptocurrency investments or requests for more payments to release funds

from seemingly legitimate platforms. In pig butchering scams, fraudsters slowly build a relationship of trust through online communication, luring victims into a fake cryptocurrency investment. Victims are tricked into gradually increasing their investment, often over weeks or months. Unlike one-time scams, these schemes involve multiple, growing payments, making early detection critical. Recognizing signs of fraud after the first suspicious transaction and stopping further investments can significantly limit a victim's financial loss, highlighting the crucial role of timely alerts from crypto exchanges in preventing further victimization.

Sample Notification

Subject: Security Alert: Your Transaction May Be At Risk

Dear [User],

We've noticed unusual activity in your recent transaction that raises concerns. At [Exchange Name], your security is our priority. We urge you to be vigilant for signs of fraud, including:

- Unsolicited Investment Offers: Beware of new online acquaintances who ask you to invest/donate/loan them money, and cannot meet in person until after you send them money.
- Promises of High Returns: Offers guaranteeing high returns with little risk are hallmark signs of Ponzi schemes.
- Pressure to Act Quickly: Scammers often create a sense of urgency to cloud judgment.
- Requests for More Payments: Be cautious of demands for additional funds to unlock or withdraw investments.
- Threats or Blackmail: Sextortion scams involve threats to release personal information unless you pay.

If you recognize any of these signs, please halt further transactions and contact us immediately for support.

Best regards,

[Your Exchange's Security Team]

- **Sharing crypto addresses linked to fraud:** Virtual asset platforms have the opportunity to enhance user safety by sharing information on cryptocurrency addresses linked to fraud. This collaborative effort can alert users about risky transactions before they occur, further protecting them from potential scams. When a user inputs the destination blockchain address for a withdrawal, the virtual asset platform would screen that address against a list of blockchain addresses that have been flagged by peer virtual asset exchanges.

- **Measure the ROI of fraud prevention.** Trust and Safety teams within companies could evaluate the economic impact of allowing scammers on their platforms. Assessing the costs associated with fraud, from impact on user retention to broader reputational damage, can highlight the importance of investing in robust anti-fraud measures to their organizations' senior leadership.
- Public sector could **create additional incentives for businesses** to prioritize protecting their customers against fraud and scams.
    - Governments could enact legislation or introduce new regulatory requirements **mandating that communication entities, including social media platforms, messaging services, telecommunications companies, and dating applications, implement comprehensive fraud prevention initiatives**. These initiatives could encompass a safe harbor provision to: 1) lawfully enable and encourage the cross-platform sharing of intelligence on fraudulent accounts, 2) the prompt and proactive elimination of accounts operated by users conducting fraudulent activities; and 3) the integration of cautionary alerts within chat interfaces triggered by specific conversational indicators.
    - Governments could take cues from the UK's handling of Authorized Push Payment (APP) fraud and the implementation of the Contingent Reimbursement Model (CRM) Code, demonstrating a commitment to protect consumers by establishing a framework for reimbursement in specific fraud scenarios.
    - Governments could **organize legislative hearings** with dating sites and social media companies to tackle online fraud. This forum would highlight the challenges and trends in scams, assess the effectiveness of current defenses, and explore new protective measures. Such a hearing could drive stronger regulatory frameworks and foster cooperation between the tech industry and policymakers to better safeguard consumers against fraud.
    - **Government agencies can encourage private sector entities** to invest in protecting users against fraud, by publicly praising their work or writing to senior leadership.

Add friction to high-risk transactions

Description

Introduce obstacles that slow down or block authorized transfers that might be fraudulent, particularly within the context of Pig Butchering scams.

Obstacles

- **Insufficient financial incentives to block authorized fund transfers.** In the United States, regulations like the Electronic Fund Transfer Act (EFTA) and Regulation E, overseen by the Consumer Financial Protection Bureau (CFPB), ensure that consumers are protected from unauthorized electronic fund transfers, including those caused by fraud, and require financial institutions to promptly investigate and reimburse consumers for any losses resulting from such transactions, provided they are reported within 60 days of appearing on the account statement. As such, banks in the US invest in fraud detection controls and secure authentication systems to prevent *unauthorized* withdrawals. While banks have a clear financial incentive to prevent unauthorized transactions, they lack a similar incentive to halt authorized fund transfers, where victims willingly authorize a transfer to scammers. This discrepancy creates a challenge in addressing various types of fraud, such as pig butchering, romance fraud, investment schemes, and sextortion, where victims initiate the transfer themselves.

Opportunities

- **Align incentives by requiring financial institutions and social media to reimburse victims of Authorized Push Payment (APP) fraud.** Authorized Push Payment (APP) fraud occurs when individuals are tricked into authorizing the transfer of money from their own account to an account controlled by a fraudster. Unlike unauthorized transactions, where payments are made without the account holder's consent, in APP fraud, victims are typically fooled into transferring funds to the fraudster voluntarily. This type of fraud often involves convincing victims through various deceptive means, such as impersonating a legitimate entity or manipulating emotions, resulting in financial losses to the victim. Governments could consider adopting a framework similar to the UK's Contingent Reimbursement Model (CRM) Code, which establishes standards for

banks to reimburse victims of authorized push payment (APP) fraud. This aligns banks' incentives to reduce fraudulent transactions, even when victims directly authorize the transaction. The onus to reimburse could also be shared between the financial institution and the communications platform where the fraud was initiated.

- **Virtual asset service providers could require additional verification at the point of fund transfer.** VASPs can strengthen their fraud prevention measures by introducing enhanced verification processes during fund transfers, exemplified by the UK's Confirmation of Payee (CoP) program. Some banks are experimenting with technologies that require consumers to verify the identity of the receiving party before executing the transfer. While implementing such initiatives in the virtual asset realm poses challenges due to scammers' ability to create new blockchain addresses, virtual asset exchanges can leverage blockchain intelligence tools to analyze withdrawal destination addresses. These tools can flag high-risk addresses with no prior activity or connections to scams, providing users with alerts to mitigate potential risks.
- **Virtual asset service providers could implement a mandatory cool-down period** before allowing any outgoing transactions from a newly created account. This buffer period would give users time to reconsider transactions and potentially identify any red flags.

Take down fraudsters' accounts

Description

Communication platforms (social media, messaging, dating) have the opportunity to invest in the removal of scammer accounts from their platforms, thereby enhancing user safety and trust.

Obstacles

- Social media and messaging companies often emphasize the **challenges in filtering and screening scammer accounts** due to the sheer volume and ever-changing tactics of scammers. They also stress the importance of minimizing false positives, where legitimate users' accounts are mistakenly taken down. Furthermore, some messaging applications utilize end-to-end encryption, limiting the use of conversational indicators, such as references to investment schemes or scam domains, to identify potential fraudsters.

Social media platforms may **lack immediate financial incentives** to take proactive action against scammer accounts.

Opportunities

- Governments could **create regulatory and financial incentives for social media and other companies to take down fraudsters' accounts**. In the UK, social media platforms are now obligated to address scammer accounts due to the requirements set forth by the Online Safety Act. The act establishes a new "duty of care" for online platforms, compelling them to address both illegal and harmful content posted by users. Failure to fulfill this duty could result in fines of up to £18 million or 10% of their annual turnover, whichever is higher.
- **Firms can sign the** Online Fraud Charter, which outlines commitments to combating online fraud. Notably, platforms like Facebook, LinkedIn, and Match Group have signed the charter, further underscoring their responsibility to take proactive measures against fraudulent activities on their platforms.

Take down fraudsters' domains

Description

Taking down domains in bulk, in near real-time.

Obstacles

- **Rapid Domain Registration:** Fraudsters can easily register new domains quickly, making it difficult to keep up with the constant churn.
- **Verification Challenges:** Domain registrars and hosting providers require evidence of fraudulent activity before taking down a site, which can be time-consuming to gather for a large number of domains.
- **Jurisdictional Issues:** Fraudsters may operate from countries with lax regulations, making legal action to seize domains complex and slow.

Opportunities

- **Automated Detection & Reporting:** Technology firms can develop AI-based solutions to automatically identify websites linked to investment schemes and

other fraud schemes. This allows for automated reporting of large numbers of domains to registrars and hosting providers.

Disrupt organized crime groups with offensive cyber operations

Description

Where appropriate, governments should consider offensive cyber operations to disrupt the operations of transnational organized crime groups (TOCs) involved in pig butchering.

Obstacles

- **Navigating the Gray Zone:** Offensive cyber operations can occupy a legal and ethical gray zone. Balancing the need to disrupt fraud with upholding international norms and respecting digital sovereignty requires careful consideration.

Opportunities

- **Leverage the cyber capabilities** of the Five Eyes alliance to target transnational organized crime groups involved in pig butchering.
- Collaborate with governments seriously impacted by fraud syndicates to **disrupt key infrastructure they rely on**. This could involve:
    - Targeted Infrastructure Disruption: Thai telecommunication companies could, with proper legal authorization and regulatory incentives, limit access to specific IP addresses associated with known scam compounds operating in Myanmar
    - Visa Revocation: Countries could revoke visas of individuals identified as key players within syndicates (including TOC co-conspirators in regional governments), hindering their ability to travel and conduct operations internationally.

Share information between businesses to better block fraudsters

Description

Firms can share data on fraudsters with each other to better take down their accounts, and block fraudulent fund transfers.

Obstacles

- **Data privacy regulations discourage information-sharing for fraud prevention:** In-house legal teams often prioritize compliance with data privacy regulations such as GDPR over proactive fraud prevention measures. Concerns about potential fines and legal repercussions discourage these teams from sharing identifiable information about potential fraudsters with other businesses, leading to a reluctance to engage in collaborative data sharing initiatives.
- **Finding the right technology provider can be daunting**. Government-built software solutions may face hurdles such as slow development. Identifying private sector solutions that work for a network of entities can be difficult.
- **In the US, Sections 314(a) and 314(b) of the USA PATRIOT Act are not fully utilized.** Many financial institutions fail to engage in the voluntary provision of 314(b) or do so selectively, limiting its safe harbor benefits. Additionally, 314(a) is often ineffective for law enforcement due to its slow pace and lack of a feedback mechanism for financial institutions.

Opportunities

- **Provide legal aircover to share information associated with fraud.** To encourage the sharing indicators associated with fraud (e.g., account handles, email addresses, blockchain addresses) between businesses, regulatory agencies can establish guidelines that offer legal protection. This guidance would enable both financial institutions and communications companies (e.g., social media, dating platforms, messaging apps, telecoms) to share such information without fear of legal consequences of breaching data privacy regulations. While in the United States, USA PATRIOT Act Section 314(b) permits financial institutions to share information with each other to better detect money laundering or terrorist activity, this has shortfalls including limited to financial institutions, voluntary, and not explicitly designed for fraud

prevention. Regulatory sandboxes or explicit directives could clarify expectations for businesses to collaborate in sharing this information and expand the scope of businesses to include communications businesses.

- Corporations should contemplate **incorporating clauses in their Terms and Conditions or Privacy Notices**, explicitly permitting the sharing of information regarding criminal activities provided specific criteria are fulfilled.
- **Create greater incentives for information-sharing.** Governments could enact legislation or introduce new regulatory requirements mandating that communication entities–including social media platforms, messaging services, telecommunications companies, and dating applications–to share intelligence on fraudulent accounts to enable faster and more effective takedown of fraudster accounts.
- **Mandate financial institutions to share intelligence on fraud.** In the United States, the government ought to explore updating both 314(a) and 314(b). Regulatory bodies should offer clear directives explicitly permitting financial institutions (FIs) to utilize 314(b) across all forms of fraudulent financial transactions. Furthermore, there should be public discourse regarding the possibility of mandating engagement with 314(b) and establishing a framework for scalable proactive measures using privacy-enhancing technologies. Modernizing 314(a) should focus on improving response times and implementing a feedback mechanism to reduce false positives.
- **Governments could develop digital platforms for information-sharing.** For instance, the Monetary Authority of Singapore (MAS) recently launched COSMIC, a digital platform that allows financial institutions to securely share with one another to detect and deter criminal activity, in partnership with six major commercial banks in Singapore.
- **Businesses could utilize private technology solutions to facilitate lawful and widespread cross-industry sharing of information** pertaining to fraudulent activities.
    - Communications companies (e.g., social media, dating platforms, messaging applications) could share data with each other to accelerate takedown of fraudster accounts (e.g., names, phone numbers, email addresses, IP addresses, device IDs).
    - Crypto exchanges, communications companies, and law enforcement could share blockchain addresses linked to fraud with each other to facilitate more effective screening of fraudulent deposits and withdrawals.
    - Communications companies could share data on fraudster accounts with law enforcement to enable more effective seizures and disruptions.

- Companies could **establish joint ventures** to facilitate information-sharing on fraud, as exemplified by Transactie Monitoring Nederland B.V. (TMNL). Founded in 2020 by five Dutch banks, TMNL consolidates transaction data from various banks to provide valuable insights into potential money laundering and terrorist financing activities.
    - **Non-profits could be created to facilitate information-sharing**. Cifas, for instance, is a UK-based non-profit fraud prevention service that facilitates the sharing of fraud-related information among its members, including financial institutions and retailers, to prevent fraudulent activity such as identity theft and account takeover fraud. The National Cyber-Forensics & Training Alliance (NCFTA) in the US follows a similar model of facilitating information-sharing between its members. GARP, through its subsidiary FCi2, is utilizing privacy-enhancing technologies for sharing critical fraud-related intelligence among institutions, safeguarding customer information in the process.

II. PURSUE ACCOUNTABILITY

Seize illicit crypto assets at custodial exchanges

Description

- Law enforcement traces, freezes, and seizes fraud proceeds at crypto exchanges where fraudsters cash out.

Obstacles

- **Quick Liquidation**: Fraudsters often liquidate assets before victims realize and report the fraud, complicating asset recovery. In pig butchering scams, perpetrators gradually gain their victims' trust, drawing them into fraudulent cryptocurrency investment schemes. The deceitful tactics result in victims incrementally increasing their investments over weeks or months. This extended timeframe means that by the time victims recognize the fraud and report it to law enforcement, the fraudster often already liquidated most of the invested funds, complicating efforts to freeze, seize, and recover the losses.
- **Profitable Despite Seizures:** Pig butchering scams remain profitable despite asset seizures.
- **Non-cooperative Exchanges**: Some exchanges may not comply with law enforcement requests to freeze funds.
- **Non-cooperative Financial Systems:** Due to the significant revenue from pig butchering going to state-embedded malign actors in countries like Cambodia, incentives are not aligned for domestic financial systems to collaborate in good faith with international investigations
- **Bandwidth Constraints:** In many jurisdictions, the volume of cases exceeds law enforcement's capacity.
- **Legal Limitations:** Law enforcement may lack authority to seize digital assets.
- **Detection Challenges:** Crypto exchanges may not recognize deposits as fraud proceeds.
- **Nested Exchanges:** Scammers are exploiting a compliance gap where nested exchange account holders, dependent on larger exchange liquidity pools, evade Know Your Customer (KYC) scrutiny. While the larger exchanges vet nested

exchange operators, nested exchanges may neglect KYC procedures for their own customers. This arrangement also relieves the custodial exchange from the responsibility of monitoring or reporting the true nature of the transactions by depositors.

Opportunities

- **Allocate additional resources to establish or enhance dedicated law enforcement task forces specialized in combating online fraud.** Federal agencies should consider creating and funding these units to enhance the real-time identification and seizure of fraudulent proceeds. Drawing inspiration from initiatives like Australia's Joint Policing Cybercrime Coordination Centre (JPC3), which received $89 million in funding in 2022, these units can bring together law enforcement officers from various levels of government and collaborate with international partners and private sector experts. By adopting a comprehensive approach that covers prevention, pursuit of cybercriminals, and victim support, these task forces can effectively combat cybercrime. In the United States, agencies that meaningfully participate at the National Cyber Investigative Joint Task Force (NCIJTF) could receive increased funding and the NCIJTF could expand its role as a fusion center to lead interagency investigations targeting cyber threat actors. Additionally, the U.S. Secret Service's Cyber Fraud Task Forces (CFTFs), aimed at disrupting financially motivated criminal groups, could expand with more funding to address evolving global threats adequately.
- **Enhance the capacity and capabilities of state and local law enforcement agencies.** These agencies could invest in tools and training to expedite the tracing and freezing of cryptocurrency transactions on exchanges. The National Computer Forensics Institute (NCFI) in the United States plays a crucial role in building these capabilities at the state and local levels and could receive additional funding to train and equip law enforcement personnel accordingly to relieve the financial burden on local communities.
- **Screen Deposits' Source of Funds:** By employing blockchain analytics tools and reporting platform APIs like Chainabuse, crypto exchanges can analyze deposits' source of funds to identify and flag potential proceeds of fraud.
- **Pursue non-compliant exchanges:** Regulatory agencies can take enforcement action against unlicensed money services businesses and exchanges that fail to implement sufficient anti-money laundering (AML) controls that block crypto proceeds of fraud from cashing out of their platform.
- **Pursue financial networks of Transnational Organized Crime groups:** A strategy shift is needed to effectively impact the profitability of industrial-scale

fraud schemes: moving from isolated case investigations, which only recover funds for a few victims and do little to impact the profitability of fraud, to broad, systematic efforts aimed at the financial networks of the transnational organized crime groups behind these scams. This approach includes freezing their assets across cryptocurrency exchanges and traditional banking institutions, more effectively targeting the profitability of their operations.

- **Legal Reforms That Empower Law Enforcement to Seize Digital Assets**: In the United States, as seen in the UK's implementation of the Economic Crime and Corporate Transparency Act (ECCTA) and the Criminal Finance Act, potential legal revisions could strengthen federal law enforcement's capacity to confiscate digital assets such as cryptocurrencies, bringing them more in line with the seizure of cash and conventional monetary instruments. These adjustments could involve increasing or eliminating the $500,000 threshold for civil administrative forfeiture, similar to cash or monetary instruments today. Moreover, acknowledging that blockchain assets are ubiquitous, law enforcement could have increased ability to legally seize blockchain assets, even if the asset controller is located in a foreign jurisdiction.
- Enable law enforcement, exchanges, and victims, and to mark addresses as linked to pig butchering so exchanges can see this information

Seize illicit crypto assets on non-custodial accounts

Description

- Law enforcement agencies can work alongside issuers of stablecoins and other digital assets to freeze assets derived from ‘pig butchering’ and other fraud schemes.

Obstacles

- Criminals might shift to using stablecoins and other assets that are difficult or impossible to trace, and that cannot be frozen, to avoid detection and seizure.

Opportunities

- Regulatory bodies could **establish rules encouraging the use of traceable and freezable stablecoins**. Criminals prioritize stablecoins for their price stability, availability on on-ramps and off-ramps, liquidity, and low transaction fees,

often opting for widely-used stablecoins on blockchains with low transaction fees, such as Tether (USDT) on the TRON blockchain. However, given Tether's recent cooperation with authorities to freeze illicit funds, criminals may move towards non-freezable stablecoins like DAI. Regulators could require virtual asset service providers to perform thorough risk assessments on assets they list, focusing on traceability and the ability to freeze assets. For example, the New York State Department of Financial Services (NYDFS) has a specific process for the listing of virtual currencies, including stablecoins, by licensed entities. Only those stablecoins that have been pre-approved and "greenlisted" by the NYDFS can be readily listed and offered to customers by these entities. This greenlist represents a curated list of cryptocurrencies that have met the regulatory standards set by the NYDFS, ensuring they comply with the state's legal and regulatory requirements.

Seize fiat assets in commercial and investment banking accounts.

Description

- Significant withdrawals from investment or brokerage accounts belonging to victims are typically transferred through conventional fiat currency channels.

Obstacles

- Commercial and investment bankers often lack sufficient education about investment scams and other cyber-enabled fraud schemes. Limits imposed by custodial exchanges on large dollar deposits lead high-dollar loss victims to directly wire funds to bank accounts controlled by fraudsters.

Opportunities

- **Enhance Education and Awareness**: Partner with organizations such as the American Bankers Association to provide targeted training and awareness programs for commercial and investment bankers. By educating bankers about the intricacies of investment scams and cyber-enabled fraud schemes, they can better identify suspicious transactions and take appropriate action to prevent victim losses.

Identify and arrest key perpetrators

Description

- Comprehensively map the criminal networks behind the industry and arrest key perpetrators where possible.

Obstacles

- **Insufficient Focus:** Many investigations focus on recovery for individual victims versus arresting key perpetrators. Building a case on a pig butchering syndicate as a whole and its supporting infrastructure within a host government requires significant investigative resources.
- **International Challenges:** Jurisdictional limitations and profoundly compromised law enforcement infrastructure in certain countries (e.g., Myanmar, Cambodia) can hinder arrests.
- **Hydra Problem:** Even if a single investigation leads to arresting one key target (e.g., one mule, or one money launderer), the syndicate continues operating and is frequently protected by major local power brokers.
- Law enforcement agencies occasionally place an emphasis on on-chain tracing in their investigative endeavors, potentially overlooking essential **off-chain investigative methods** such as search warrants crucial for constructing successful cases leading to prosecution.

Opportunities

- **Prioritize fraud at the national level.** For instance, the U.S. government—including the White House, Department of Justice, and Congress—should consider making online fraud prevention a national priority, similar to the efforts against terrorism financing and ransomware. This could involve Congress earmarking funds specifically for anti-fraud initiatives within law enforcement agencies, or creating infrastructure for the Department of State to "own" the issue through the lens of organized crime. The US and other nations could look to the UK's proactive approach in prioritizing fraud prevention at the national level. In May 2023, the UK government announced tackling fraud a priority for all police forces across the UK, recognizing that fraud accounts for over 40% of all crime but receives less than 1% of police resources. UK initiatives such as the creation of a national Fraud Strategy, the

Online Safety Bill, the Global Fraud Summit, and a National Fraud Squad (NFS) dedicated to pursuing the most sophisticated and harmful fraudsters, with over 400 new specialist investigators, serve as a blueprint for coordinated cross-government action.

- Promote law enforcement's utilization of established Task Forces and **inter-agency collaboration** to develop comprehensive investigations that result in more indictments, shifting the focus away from investigations primarily aimed at recovering money.
- **Unsealed Indictments:** Unsealing indictments against foreign nationals that cannot be immediately arrested (including high-level complicit government officials) serves to send a strong message, disrupt criminal operations, and lay the groundwork for future arrests, despite jurisdictional challenges.
- **Targeted Apprehensions:** Prioritize high-value targets within syndicates, including syndicate leaders, money launderers, tech specialists, and elite state-embedded criminals.
- **Red Notices and Global Cooperation:** Leverage Interpol's Red Notice system to request international arrest warrants for top syndicate leaders. This can pressure countries to cooperate and disrupt operations.
- **Bilateral Cooperation:** Establish joint training programs and bilateral investigations centers to improve coordinated responses.
- **Pursue opportunities for mutually beneficial collaboration with China:** US and other countries could consider collaborating with China to tackle pig butchering given their multi-layered interest in addressing this issue.

Sanction key criminals and their co-conspirators

Description

Utilize targeted sanctions to disrupt international criminal groups and their co-conspirators in host governments, hindering their ability to travel and access funds

Obstacles

- **Evolving Networks:** Fraudsters may use complex financial networks and shell companies to obfuscate ownership and evade sanctions.

- **Tipping off the target:** Imposing sanctions before an indictment is unsealed can risk tipping off the target and jeopardizing ongoing investigations.
- **Diplomatic Risk:** In Cambodia particularly, the owners of the compounds where pig butchering is occurring at scale are amongst the most powerful people in the country. Diplomatic missions are loathe to disrupt the bilateral relationship by targeting them.

Opportunities

- **Synchronized Sanctions**: Where appropriate, aligning sanctions with public indictments can strengthen the overall impact of the desired change in behavior, thereby providing a more robust deterrent.
- **Targeted Sanctions:** Designate high-profile fraudster, syndicate leaders, and elite state-embedded malign actors–restricting their access to financial services, including bank account freezes, asset seizures, and travel restrictions–and, where the evidence justifies it, also proceed against them criminally.
- **Sanctions Leads to Greater Private Sector Action:** Sanctioning transnational organized crime groups could push social media platforms, dating apps, and messaging apps to scrutinize related accounts more closely as part of their sanctions compliance program. This could expand the fraud problem for businesses from a "Trust and Safety issue" to a "Sanctions Compliance issue", which may lead to greater investment.

III. EMPOWER PEOPLE

Proactively build awareness about scams and fraudulent recruiting

Description

Increase public knowledge about the various types of scams and fraud as well as the abusive recruiting/trafficking practices, ensuring widespread understanding across different demographics both up and downstream.

Obstacles

- **Unproven Efficacy**: The effectiveness of such educational campaigns in actually reducing fraud is not well-established, underscoring the need for further research. For example, a study by Danish and Dutch academics found that awareness campaigns, like the one by a significant Danish bank targeting clients over 40, showed no significant impact on reducing financial fraud, indicating a gap in understanding the direct benefits of these initiatives.
- **Adapting to New Scams**: Scammers are constantly updating their methods, which poses a challenge for keeping educational materials current.
- **Audience Reach**: Overcoming information overload to effectively reach and engage diverse audiences. It can be difficult to break through the noise.
- **Varying Audience Locations**: Different groups use different platforms, requiring tailored outreach strategies.

Opportunities

- **Diversify communication channels.** Incorporate various platforms and formats for educational content. For instance, the Federal Trade Commission (FTC) utilizes fotonovelas, a unique and visually engaging storytelling method, to educate Spanish-speaking communities about various scams and consumer protection rights. These narrative booklets, which blend compelling photos with straightforward text, cover topics like identity theft and scam awareness, making complex information easily accessible and memorable.

- **Build a recognizable brand**: Establishing a recognizable brand is crucial for effective awareness campaigns, as demonstrated by initiatives like Get Safe Online and Take Five, which have significantly contributed to educating the public about online safety and fraud prevention for 20 years and 6 years, respectively. Similar to Nike's enduring association with the slogan "Just Do It," these brands underscore the significance of consistency and longevity in driving awareness. Prioritizing the creation of a lasting brand over short-term campaigns is essential for maximizing impact and ensuring sustained engagement with the target audience.

Identify and support upstream victims

Description

Urgently improve the systems and infrastructure dedicated to identifying and supporting victims of trafficking and abuse within Southeast Asia's scam compounds.

Obstacles

- Insufficient and overwhelmed systems to support trafficking victims coming out of pig butchering compounds in Southeast Asia. The scale and direction of human trafficking flows resulting from this crime type is unprecedented. As such, the infrastructure and capacity to care for victims is tremendously overwhelmed and under-resourced, leading to multiple parallel crises.
- Combination of incentive and capacity barriers for proper and effective screening of trafficking victims coming out of pig butchering compounds in Southeast Asia. Disambiguating between criminals with agency and forced criminals is paramount. Mass arrests, charges and convictions of scam center workers will do nothing to disrupt the industry. Rather, it will re-victimize the large numbers of people who are engaged in criminal activity against their will.

Opportunities

- **Strengthen processes for human trafficking victim screening:**
    - Create/strengthen host government national identification and referral mechanisms (and consistency across countries)

    - Build capacity of embassies in destination countries to identify victims and report the crimes committed against them
    - Build capacity of relevant units of local government agencies (specifically immigration) to identify victims
- **Strengthen and contextualize survivor services for victims of forced scamming**
    - Source governments should consider immediately increasing funding for their social service agencies supporting victim services and strengthening processes for repatriation
    - Create emergency shelters accessible by victims of forced criminality in destination countries; victims should not be detained in prisons or illegal immigration detention centers upon identification
    - Provide trauma-informed psychological, vocational, and legal support for survivors after return home
    - Ensure relevant government agents, including law enforcement, social services, judicial officials, and immigration officials are equipped in anti-trafficking and labor exploitation laws, trauma informed care, and repatriation mechanisms
- Ensure that countries which are failing to care for survivors of forced scamming or to identify victims in good faith are held accountable via policy mechanisms such as the State Department's Trafficking in Person's Report and related authorized sanctions.

Identify and support downstream victims

Description

Provide victims with an opportunity to report this crime into a framework that is user-friendly and captures relevant data. Set reasonable expectations for recovery of funds and prosecution of suspects. Establish resource portals with vetted information and legitimate support programs.

Obstacles

- Unstructured and Incomplete Victim Reports: Many victim reporting systems do not collect structured information needed in crypto investigations such as scammer blockchain addresses, and crypto payment transaction hashes.

Moreover, victims often do not report enough information or they report wrong data that needs to be cleaned..

Opportunities

- **Improved Reporting Systems:** Governments are investing in improving reporting systems, like the FBI's IC3 and the UK's Action Fraud, to be more user-friendly and capture the necessary data for investigations. Reporting portals could be designed to collect information specific to pig butchering, enabling law enforcement the best opportunity for triage and recovery.
- **Link to Reporting Platforms from Online Platforms:** Crypto exchanges, wallets, and social media applications can link to victim reporting platforms such as Chainabuse and IC3 to shorten the time between victimization and report.
- **Identify connections between victims to build larger cases.** Victim reporting platforms can leverage network analysis to identify connections between different victims. Chainabuse, for instance, identifies instances in which multiple victims' are connected through common scammer indicators (e.g., phone number, social media handle) or cryptocurrency transactions. These insights enable law enforcement to pursue larger cases with multiple victims.

Acknowledgements

We are grateful to experts at the following organizations for leading the fight against pig butchering and providing insights into the obstacles and opportunities in the fight against pig butchering and other forms of online fraud.

- Joby Carpenter, ACAMS
- PJ Rohall, About Fraud

- Kathy Waters, Advocating Against Romance Scammers
- Aidan Larkin, Asset Reality
- Alona Katz, Brooklyn District Attorney's Office
- Saskia Parnell, BMO
- Jackie Burns Coven, Chainalysis
- Erin Plante, Chainalysis
- Jennifer Chapin, Commodity Futures Trading Commission
- Melanie Devoe, Commodity Futures Trading Commission
- Matthew Hogan, Connecticut State Police
- Ally Armeson, Cybercrime Support Network
- Karissa Brumley, Cybercrime Support Network
- Kim Casci-Palangio, Cybercrime Support Network
- Nicola Staub, CYBERA & SCAM:help
- Kevin O'Connor, FinCEN
- Karen Helmberger, FS-ISAC
- Al Pascual, Scamnetic
- Jorji Abraham, Global Anti Scam Alliance
- Brian Bruce, Global Anti-Scam Organization
- Mina Chiang, Humanity Research Consultancy
- Benedict Hamilton, Kroll Associates
- Matt Friedman, the Mekong Club
- Hailey Windham, Mission Omega
- Ayelet Biger-Levin, Scamrangers
- Martin Burke, South Australia Police
- Rachel Lerner, FCi2
- Carmen Corbin, United Nations Office on Drugs and Crime
- John Wojcik, United Nations Office on Drugs and Crime
- Kali Schildecker, United States Secret Service
- Shawn Bradstreet, United States Secret Service

- Carina Peritore, victim expert
- Amanda Wick, Women in Cryptocurrency
- Adrian Cheek, Coeus
- Lisa Plaggemier, National Cyber Security Alliance

We would also like to thank the UK Home Office for their pioneering work in defining a comprehensive national fraud strategy ("Fraud Strategy: stopping scams and protecting the public") and hosting the Global Fraud Summit, which led to many insights in this report. We leveraged their strategy framework of "Block Fraud; Pursue Fraudsters; Empower People" in organizing the various tactics outlined in this paper.