Fraudsters Bringing Home the Bacon

The Pig Butchering Scam

This latest super scam puts a modern twist on romance fraud, wherein criminals extort money from unsuspecting targets. These scammers have gotten more inventive to increase gains.

Crude as it is, “Pig Butchering” is a term used for fattening the pig before going in for the kill. Scammers groom their targets to invest in cryptocurrencies or online gaming through sham websites controlled by their gang of fraudsters. Once victims invest enough money, the scammers take it all and vanish.

The romance-meets-investment scam has become so lucrative that it has prompted alerts from authorities, including Interpol and the FBI. The latter recently released **public service announcement** warning that individual losses from these schemes can range from tens of thousands to millions of dollars.

WHITEPAPER

Maya Shabi
Payments & Risk Specialist, EverC

Securing ecommerce growth with trust and confidence

everc.com

Pig Butchering: The super scam

1. **Scammers create fake personas and initiate relationships** with a suitable victim – the proverbial "pig" – on dating sites, social media, or even random messaging masquerading as a wrong number.

2. After maintaining contact and earning the victim's trust, they **persuade targets to deposit money in digital asset wallets,** such as Coinbase, which are legitimate businesses.

3. **They then coax their targets to connect the funds** to falsified cryptocurrency investment websites and apps, fake brokers or liquidity mining pools (apps that are decentralized). Scammers can use "Virtual Dealer" plug in to crypto trading platforms in order to simulate account balances, profits or losses - fabricating market performance.

4. Once victims join the platform, **fraudulent hosts begin stimulating trades that appear to be generating profits.** Scammers may even allow their victims to withdraw some "gains" to boost the legitimacy of their operation and allay suspicion.

5. Moving forward with more confidence in their investments, **victims invest larger sums of money at the behest of their trusted scammer.** Over time, the scammer continues to manipulate victims to keep them investing more and more – otherwise known as "fattening the pig".

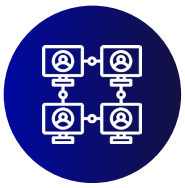
6. At a certain point, the victim feels they've had enough **and attempts to withdraw their funds from the platform, which will inevitably have an "error" or inform victims that fees or taxes need to be paid** in order to cash out.

7. **Fraudsters and their platforms then disappear with victims' cash.** Given that the transactions were done through blockchain tech, the stolen funds are nearly impossible to recover.

Pig Butchering Typologies

Fake investment websites and apps

Fake brokers on trading platforms



Fake liquidity mining pools (decentralized apps)

Group investment

Gambling

The UK: A prime location for shell companies used for scam operations

According to a study conducted by **The Bureau of Investigative Journalism,** shell companies registered in the UK are being used by Chinese criminal syndicates to carry out pig butchering operations. Scammers set up shell companies simply by selecting a UK-based property without any genuine ties to the addresses where they claim to be based. In one instance, the study found that "virtual squatters" registered more than 200 companies to a single two-bedroom apartment in east London, unknown to the actual resident. Indicating the breadth of these operations registered from the UK, investigators then compiled a list of companies likely running pig butchering schemes and were able to connect victims to countries including the UK, US, Canada, Turkey, Germany and Poland.

The ease by which Chinese-run shell companies are registered online is largely facilitated by regulatory loopholes in the UK. ID verification protocols are ambiguous for individuals using company service providers, and the cost to register can be as little as £12. Such gaps in regulation leave room for potential earnings to be laundered through the UK's financial system as shell companies are frequently used to obfuscate the true source of funds and hide their beneficial owners. Additionally, cryptocurrency exchanges and other digital assets constitute high risk for criminals to conduct money laundering operations.

To address the misuse of the UK's company register, legislators introduced the **Economic Crime and Corporate Transparency Act** to verify company registration information provided to the Companies House. The reform was only introduced in September 2022 and its actual implementation remains unclear. That said, UK authorities set a January 31 deadline for foreign owned companies registered in the UK to declare their beneficial owners in a new government registry. This constitutes part of a larger effort to tackle the approximately £100 billion in illicit financing channeled through the UK. As it stands, only 19,510 out of a total of 32,440 registered overseas organizations met the deadline.

…"virtual squatters" registered more than 200 companies to a single two-bedroom apartment in east London, unknown to the actual resident.

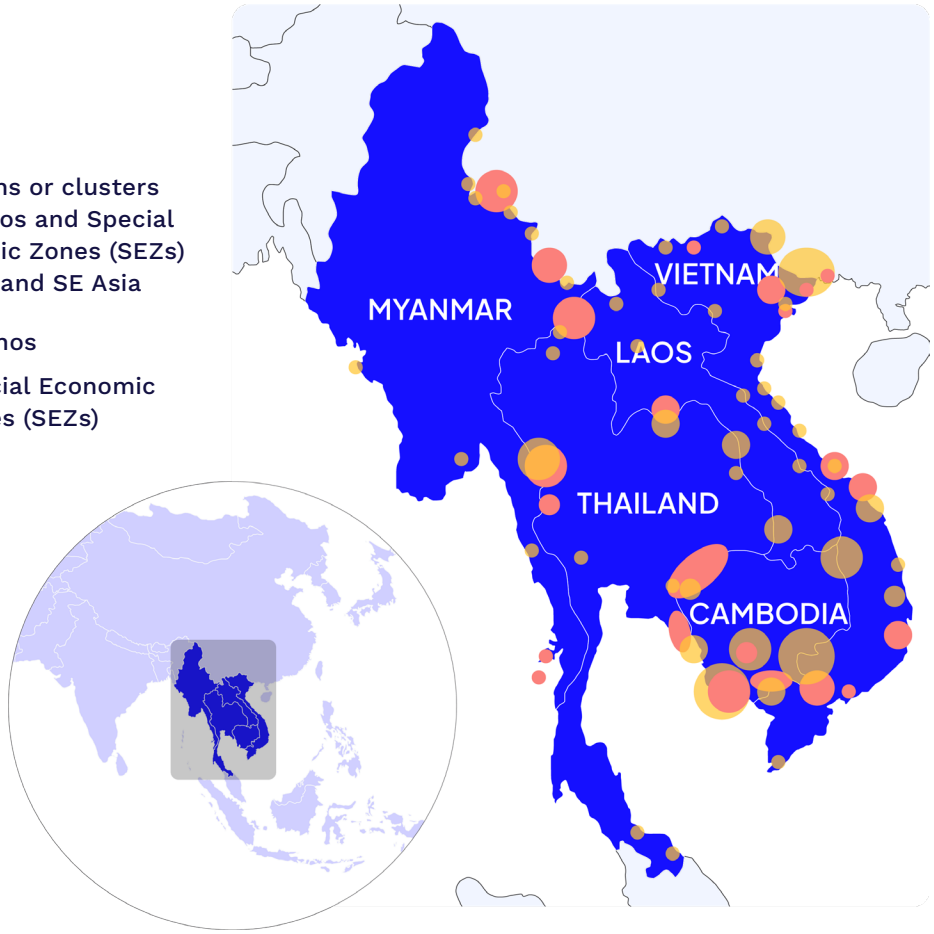
A scam propped up by human trafficking

Pig butchering is not a problem limited to fraudster networks taking advantage of financial systems and deceiving their targets. Many times, these scam operations are fueled by human trafficking – the people operating fake personas are often simultaneously victims.

Originating from China, the scamming strategy spread to organized crime groups across the globe, with particular focus on special economic zones (SEZs) across Indochina, such as Myanmar and Cambodia. People from these regional hotspots are lured by fake job advertisements to scam centers, where they're forced to perpetrate large-scale online fraud against innocent victims, often at the threat or use of extreme violence. Furthermore, trafficked persons typically have their passports and financial information confiscated by their captors to ensure that they remain stuck in the illicit cycle.

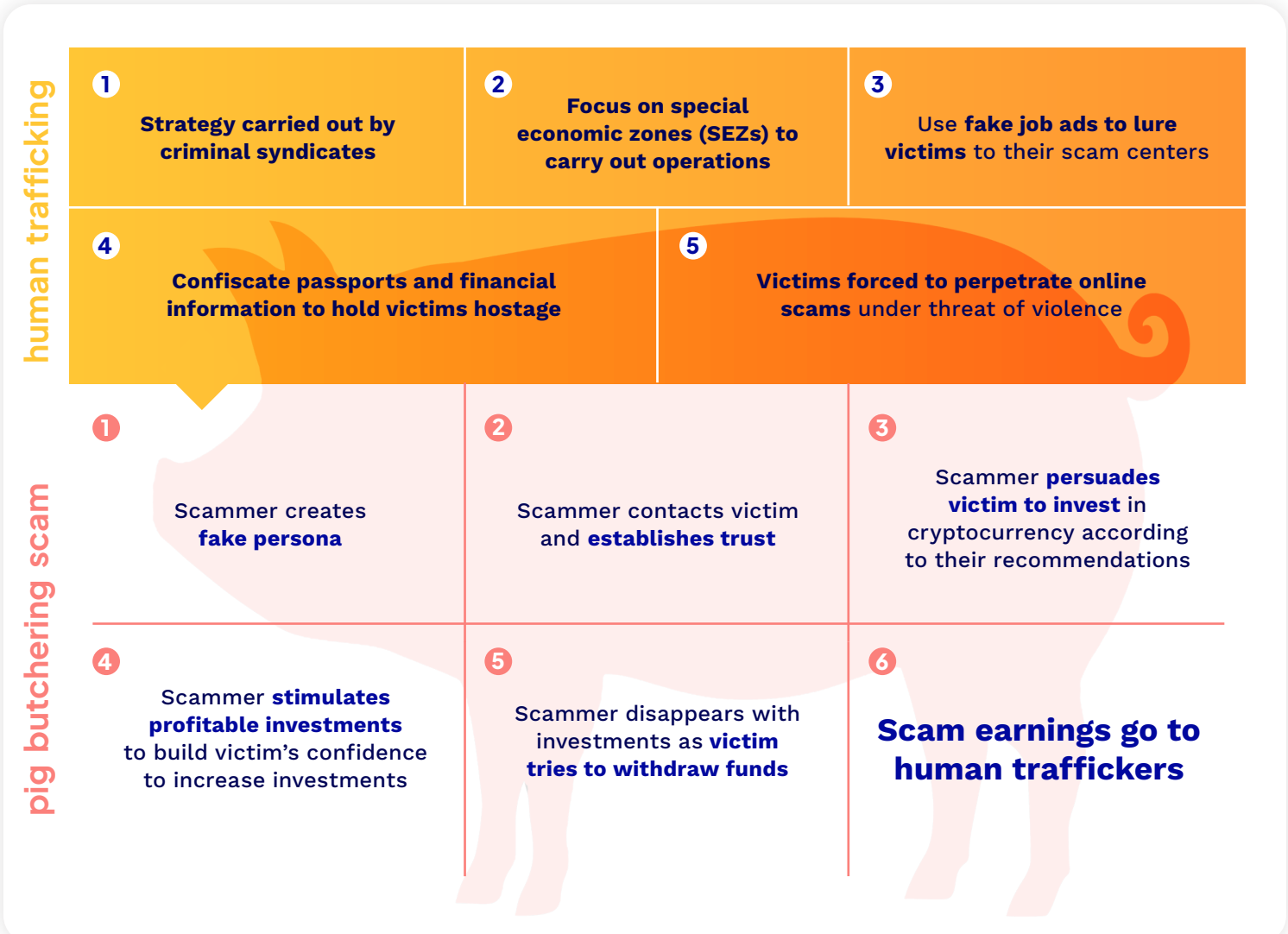
Locations or clusters of casinos and Special Economic Zones (SEZs) in mainland SE Asia

- Casinos
- Special Economic Zones (SEZs)



For example, Cambodian officials estimate that up to 100,000 people are involved in online scam centers, although repeatedly denied that the practice involved human trafficking. That was, until the US State Department downgraded Cambodia to Tier 3 in its **2022 Trafficking in Persons Report.** In November 2022, Cambodia's Interior Minister reportedly stated that authorities' efforts to crack down on human trafficking, with particular focus on Preah Sihanouk Province where its largest EEZs are located, uncovered that 95% of human trafficking complaints were indeed factual.

Several countries involved in **China's Belt and Road Initiative (BRI) are at risk for forced labor** practices by criminals seeking to exploit the trillion-dollar infrastructure development and economic integration strategy. The resulting spread of human trafficking comes, in part, from Chinese crime figures seizing the opportunity to expand their illicit enterprises abroad, providing the framework for the pig butchering industry to boom. And in recent years, the unprecedented conditions of the COVID-19 pandemic forced the Chinese gambling tourism industry to be repurposed for online scam operations, all they needed was the exploitable labor.



People from these regional hotspots are lured by fake job advertisements to scam centers, where they're forced to perpetrate large-scale online fraud against innocent victims, often at the threat or use of extreme violence.

Increasing regulatory focus

Combating human trafficking remains a top priority for authorities across the globe, and officials are seeking alternative avenues to disrupt the revenue generation from these crimes. One way is to increase regulation in the digital asset sector to limit fraudsters' access and prevent them from exploiting the online space.

Just like the pig butchering scam, digital currency trading platforms can facilitate a range of illicit activities, from small-scale scams and identity theft to money laundering and financing of terrorist networks. Lawmakers in the US are working to approve the **Digital Assets Anti-Money Laundering Act.** In the UK, the British government has **proposed a plan** to subject the cryptocurrency sector to the same oversight mechanisms as traditional finance firms. This includes establishing more thorough Know Your Customer (KYC) protocols to verify user identities, including within cryptocurrency trading platforms.

Specific to online romance scams, regulators are seeking to implement background checks and ID verification systems to ensure that users aren't duped into starting relationships with criminal actors. For example, authorities, victims, and tech companies in Australia have been hosting **national dating app roundtable talks** to tighten restrictions on who can join the online platforms. This will not only safeguard users from financial extortion but will also help protect them from possible abuse or harassment.

While increased regulation on digital assets and within online dating apps will not eliminate the practice of human trafficking, implementing stricter controls on usership within these spaces can make it more difficult for bad actors to infiltrate the payments ecosystem.

What can you do?

Raising public awareness of pig butchering has been one of the top priorities among government officials to help protect individuals from online scams. This is likely because operations based in Indochina have increased their focus on targets in Western countries, including the US and Canada.

The duty to prevent this super scam from continuing to plague internet users isn't limited to regulators. Financial institutions facilitating the transfer of digital asset payments are also responsible for protecting consumers.

In November, the **US Department of Justice** seized seven pig butchering internet domains operating between August and May 2022, which defrauded five victims out of nearly $10 million. All of these were spoofed domains from Singapore.

While authorities target and dismantle the top-tier scammers, it's important to note that these criminals operate in an interconnected environment where an abundance of other fraudulent domains exist. Put simply, for every one pig butchering domain removed, hundreds if not thousands of similar domains ready to enter the playing field and take their place.

On an individual business level, consumer protection can be fostered by implementing tighter customer verification protocols and continuously monitoring for fraudulent activity within their platforms.

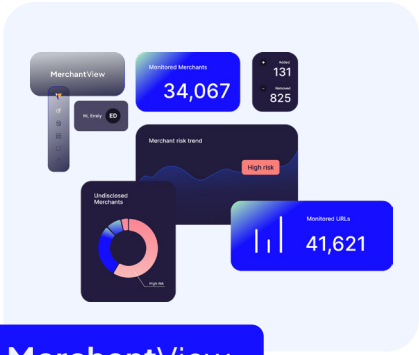
However, as financial institutions participating in the broader payments ecosystem, there lies strength in collaborating with public and private industry partners to unearth such scam networks. These measures will not only help eradicate this horrendous practice from proliferating through individual payments systems, but also further disrupt the illicit industry across the globe.

Partnering with EverC

EverC is focused on powering growth for the ecommerce ecosystem. Our automated AI-driven, cross-channel risk management solution rapidly detects high-risk merchants, transaction laundering, and illicit products, and provides ongoing monitoring to uncover evolving risks. Our team comprises domain experts in risk intelligence, open-source, deep and dark web, and online fraud detection.

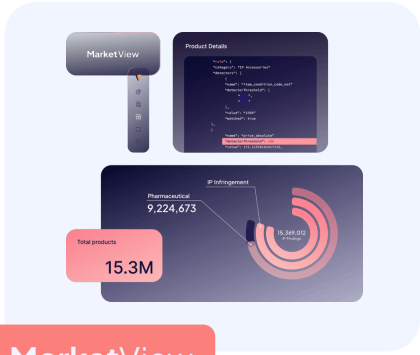
Our solutions combine artificial intelligence with expert insights, for fully integrated, customizable merchant and marketplace risk management.

EverC solutions and services provide actionable intelligence: A holistic view of the collaborative threat landscape that enables us to take down entire networks of illicit actors for safer, more successful ecommerce.



MerchantView

Merchant risk intelligence platform that uncovers money laundering and additional risk factors.



MarketView

The only fully automated solution that identifies and eliminates illicit and counterfeit products.

Risk Insight Services

Our global experts provide investigation services tailored to your risk and compliance needs.

EverC: securing ecommerce growth with trust and confidence

Learn more at everc.com