AML Watcher

Whitepaper

PIG BUTCHERING SCAM ALERT!

ARE AML LAWS READY FOR THE NEW FIGHT?

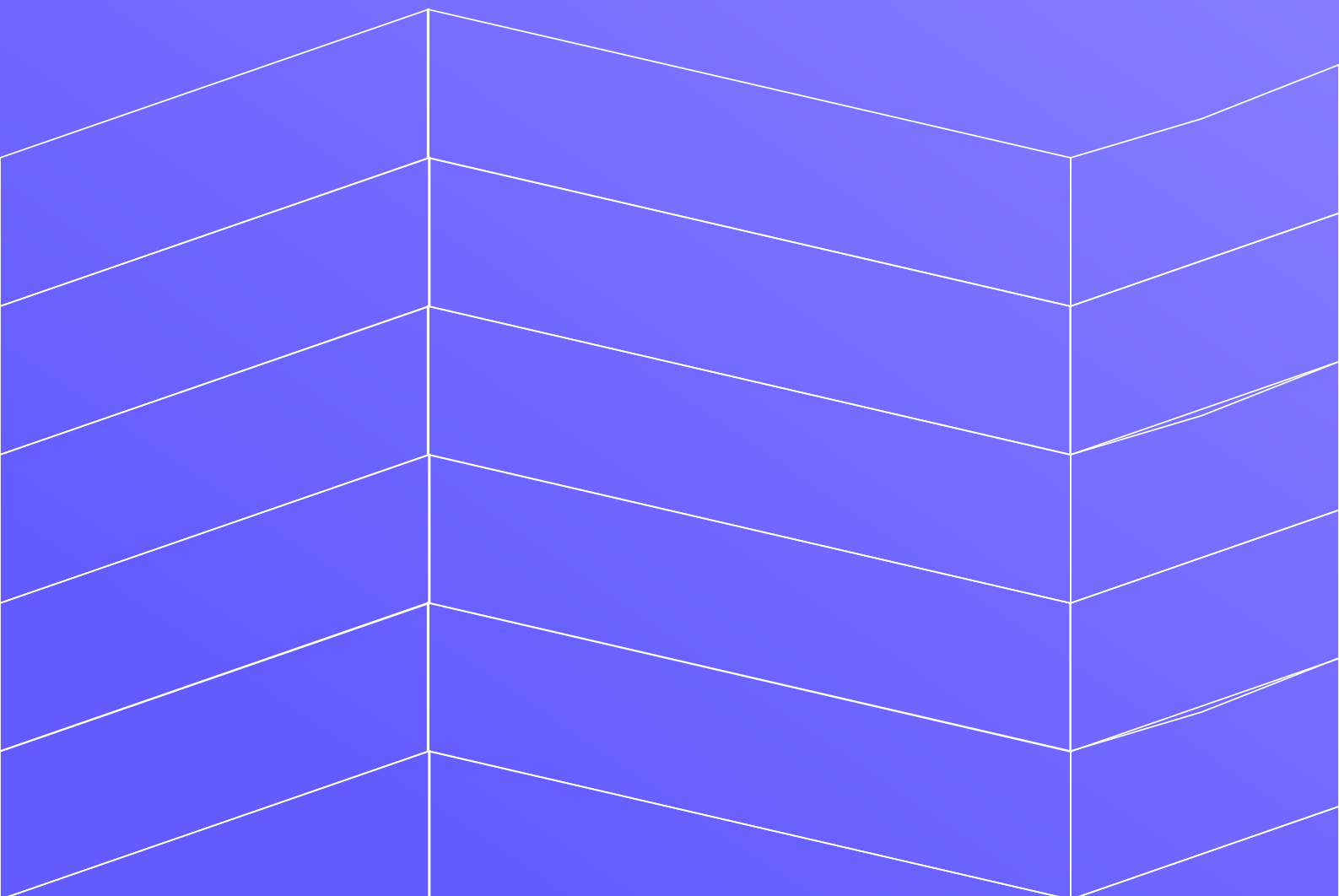


Table Of Content

Introduction

In this modern world of crime and money laundering, one particularly insidious scam has gained notoriety i.e the Pig Butchering Scam. While its name may sound peculiar, the impact of this scheme is devastating, leaving countless victims financially and emotionally shattered.

The pig-butchering scam is a new kind of cryptocurrency investment scam that is rapidly gaining traction and causing concern among security experts and law enforcement agencies.

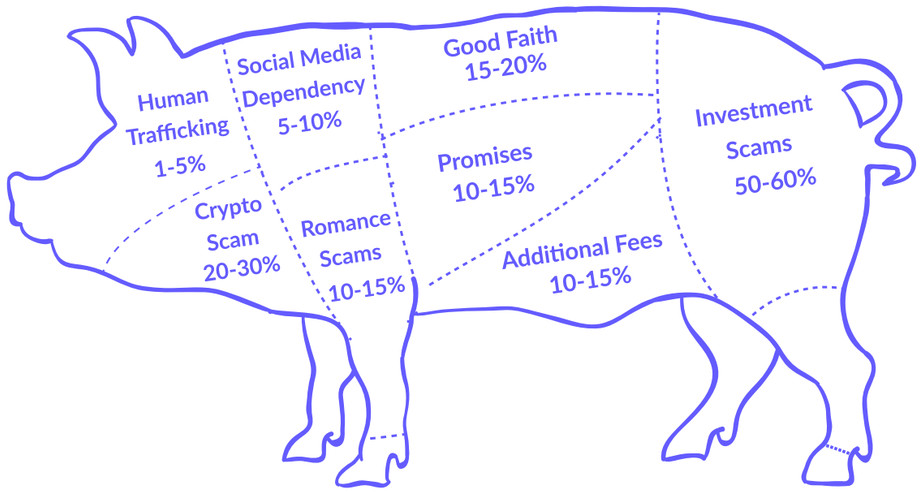
> According to the **2022 Internet Crime Complaint Center (IC3) report**, crypto-investment scams have had an unprecedented increase in both the number of victims and the total amount of losses, with the latter amounting to **US$2.57 billion in 2022.**

This e-Book delves into the nature of pig-butchering scams, how scammers carry out their operations,Warning Signs of Pig Butchering Scams, and what individuals can do to avoid falling for these fraudulent investments and dealing with massive amounts of debt.

The University of Texas at Austin's John Griffin, a professor of finance, and graduate student Kevin Mei collected the cryptocurrency addresses of almost 4,000 victims of the scam, which has been extremely popular since the outbreak. They followed the money flow from victims to scammers—who are mostly situated in Southeast Asia—using blockchain tracing technologies.

According to Griffin, a writer on financial market fraud, the criminal networks sent almost $75 billion to cryptocurrency exchanges in just four years, between January 2020 and February 2024. According to him, a portion of the amount might be the earnings from other illegal acts.

In an interview, Griffin stated, "These are sizable criminal organized networks, and they're operating essentially unscathed."



What's the Story Behind the Pig Butchering Scam?

The Pig Butchering Scam, also known as "sha zhu pan" (杀猪盘) in Mandarin, originated in China and has since spread globally. The term "pig butchering" is a metaphor used by scammers to describe fattening up their victims before slaughtering them. The scam involves building a relationship with the victim, gaining their trust, and then exploiting that trust to steal money.

Here's how it typically unfolds:The scam usually begins on social media platforms, dating apps, or even through unsolicited text messages. Scammers create fake profiles, often using attractive photos and fabricated personal details to lure in potential victims. Once contact is established, the scammer invests significant time and effort into developing a close relationship with the victim. This can take weeks or even months. They engage in frequent communication, share personal stories, and create a sense of intimacy and trust. After establishing trust, the scammer introduces the idea of investing in a lucrative opportunity. They often claim to have insider knowledge of cryptocurrency, forex trading, or other high-yield investments. They might show fabricated success stories and fake screenshots of profitable trades to convince the victim. The victim, now emotionally invested and trusting the scammer, is persuaded to invest a small amount of money initially. Seeing fabricated returns, the victim is encouraged to invest more substantial sums. The scammer may even allow the victim to withdraw small amounts to build further trust.

Once the victim has invested a significant amount, the scammer vanishes, taking all the money with them. The victim is left devastated, having lost not only their money but also the relationship they believed to be genuine.

WHAT IS PIG BUTCHERING?

PIG BUTCHERING CONSISTS OF 4 STEPS:

1. PACKAGING

Offender takes on a persona who seems wealthy & looking for friendship

2. RAISING

Scammers groom the victim, psychologically manipulating them.

3. KILLING

Scammers direct them to an investment site sending money straight to the scammer

4. CASH OUT

After a period of time, the scammer will cash out of the scam themselves

Warning Signs of Pig Butchering Scams

Recognizing the warning signs of a Pig Butchering Scam is crucial in preventing financial loss. Here are some red flags to watch out for:

Most of these scams appear ‘Too Good to Be True’. Financial firms must be cautious of investment opportunities that promise high returns with little or no risk.

Scammers often use the allure of quick and easy money to entice victims. Scammers move quickly to build an emotional connection. If someone you just met online is overly affectionate or shares personal details too soon, be wary. Furthermore, If a new online acquaintance suddenly starts giving you investment advice or insists on helping you invest, it's a major red flag. Sometimes, scammers will pressure you to invest quickly, often claiming that the opportunity is time-sensitive. Legitimate investments rarely require immediate decisions. You you want to avoid such scams, always be skeptical if the person is unwilling or unable to provide verifiable information about themselves, their job, or their investment proposal.

The Impact of Pig-Butchering Scams

The FBI's recent reports on pig-butchering scams have revealed the devastating financial impact on victims. Thousands of individuals have fallen prey to these scams, resulting in millions of US dollars in losses. However, it is possible that the true extent of the problem is even more significant, as many victims are too embarrassed to report their experiences or are unaware that they have been scammed. By closely monitoring the chat groups and identifying the fake brokerage sites, the investigative authorities were able to track down some of the cryptocurrency wallets controlled by this these scammers. Based on one group of scammers alone, we estimate that this group has netted almost US$4 million based on transactions made from January to March 2023, indicating the severity of this scam. Table 1, which shows the total amount of funds transferred to each brokerage site and their corresponding cryptocurrency wallets, gives a clearer picture of the magnitude of this operation.

Victim Demographics

One striking aspect of pig-butchering scams is the victims' demographic profile. The large transaction amounts deposited into the scammers' accounts, ranging from US$10,000 to US$100,000, suggest that the targets are not victims with limited savings. Instead, these scams appear to be targeting a more financially established demographic, including professionals with high salaries and individuals nearing retirement. Figure 13 shows that some of the transactions made to a scammer's cryptocurrency wallet were in the five- to six-figure range.

By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$3,311,742,206	Lottery/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Rensomware	$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment	$5,621,402
Identity Theft	$189,205,793	Theats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

Top reported fraud by victim losses in 2022

Source: 2022 Federal Bureau of Investigation Internet Crime Report

It is plausible that scammers are focusing their efforts on victims they consider "big fish," as these individuals are more likely to have access to large sums of money. These individuals are also potentially more susceptible to the scam because it's possible that they would like to grow their wealth and maintain their lifestyle. In some cases, these individuals might overlook red flags in their eagerness to capitalize on seemingly lucrative opportunities. According to the 2022 IC3 report, the victims of these scams typically fall under the 30 to 49 age range. This further highlights the scammers' focus on individuals with greater financial resources. Another possible target group for pig-butchering scams are individuals approaching retirement who might have substantial savings and are actively seeking investment opportunities to secure their financial future. It's possible that scammers will exploit this sense of urgency and vulnerability to convince victims to invest in their fraudulent schemes.

According to the same IC3 report, victim losses pertaining to investment fraud have reached a whopping US$3.31 billion, which is considerably higher than other types of fraud. Included in this staggering amount are complaints pertaining to cryptocurrency investment fraud, which reached US$2.57 billion last year. These alarming numbers further emphasize the importance of raising awareness and taking proactive measures against these malicious actors to protect individuals' hard-earned savings and financial futures.

How AML Laws Disrupt the Pig Butchering Scam?

Anti-Money Laundering (AML) laws play a crucial role in disrupting the supply chain that supports Pig Butchering scams. These scams often involve human trafficking, where individuals, primarily from Southeast Asia, are forced to work in cyber compounds to carry out fraudulent activities. AML regulations can help detect and prevent the flow of illicit funds that finance these operations by monitoring transactions, identifying suspicious patterns, and flagging high-risk activities.

By enforcing stricter compliance standards and encouraging financial institutions to report unusual activities, AML laws can significantly hinder the financial networks that enable these scams, thereby protecting vulnerable populations from exploitation.

What Has been the Impact of UK's Sanction Regime?

The United Kingdom has implemented a sanctions regime that targets individuals and entities involved in human trafficking and forced labor, which are often linked to Pig Butchering scams. These sanctions are part of broader efforts to combat modern slavery and other forms of exploitation. By freezing assets, imposing travel bans, and restricting access to financial services, the UK's sanctions regime disrupts the operations of those involved in these illicit activities. This approach not only serves as a deterrent but also highlights the importance of international cooperation in addressing the complex and transnational nature of scams like Pig Butchering.

Key Strategies to Avoid Pig Butchering Scams

Protecting yourself from Pig Butchering Scams involves vigilance and a healthy dose of skepticism. To safeguard your finances and emotional well-being, always verify the identity of people you meet online. Conduct reverse image searches on their profile pictures and cross-check their details on multiple platforms.

Before making any investment, thoroughly research the opportunity. Look for reviews, regulatory approvals, and credible sources of information. Be especially cautious with cryptocurrency and forex trading, as these are common areas for scams. Moreover, seek advice from financial professionals before making any investment decisions. They can provide objective insights and help you avoid falling for fraudulent schemes.Finally, maintain healthy boundaries in online relationships. Be cautious about sharing personal information and avoid discussing your finances with someone you haven't met in person.

Most importantly, if you suspect you are being targeted by a scammer, report the activity to the platform where you met them and to relevant authorities. This can help prevent others from becoming victims.

How Compliance With AML Regulations Help Prevent Such Scams?

Anti-money laundering (AML) can play a crucial role in preventing scams like Pig Butchering by targeting the financial infrastructure that scammers rely on to launder and move their illicit gains. Here's how:

01 Flag Unusal Activity

AML regulations require financial institutions to monitor transactions and report any that appear suspicious or inconsistent with a customer's normal behavior. In the case of pig butchering scams, where scammers often persuade victims to transfer large sums of money, these transactions might raise red flags. Financial institutions can flag unusual activity, such as a sudden influx of funds or large wire transfers, and report these to authorities, potentially intercepting fraudulent transactions.

02 Burst the Identity of Scammers

AML laws mandate financial institutions to implement Know Your Customer (KYC) procedures, which involve verifying the identity of their customers and understanding the nature of their transactions. These protocols help ensure that the individuals involved in financial transactions are who they claim to be. In Pig Butchering scams, where scammers often use fake identities, KYC checks can help detect and prevent fraudulent accounts from being created or used to launder money.

03 Asset Freezing and Seizure

AML laws provide the legal framework for authorities to freeze and seize assets that are suspected of being connected to money laundering or fraudulent activities. If a victim's funds can be traced and identified within the financial system, AML laws enable authorities to freeze these assets, potentially returning the stolen money to the victim and preventing the scammer from accessing it. This attempt serves as a powerful coercive measure to cut off financial gains from illegal activities.

04 Prevention of Shell Companies

Scammers often use shell companies to launder money and obscure the origin of illicit funds. AML laws that target the creation and operation of shell companies make it harder for scammers to hide their activities and launder stolen funds. By enforcing transparency in business ownership, authorities can track and disrupt the financial networks that enable Pig Butchering scams. This increased sight into shell companies can highly aid in crippling the financial lifeline of scammers.

05 Cross-Sector Collaboration

AML laws encourage collaboration between financial institutions, law enforcement, and regulatory bodies. This collaboration can lead to more effective detection and prevention of scams like Pig Butchering. By sharing information and coordinating efforts, different sectors can work together to identify and disrupt scam operations more efficiently. This joint effort can not only enhance the ability to track illicit activities but also improve the overall compliance framework.

How To Prevent Pig Butchering Scams?

Adverse media screening is an essential tool for financial institutions to identify potential risks associated with customers in high-risk jurisdictions. By scanning for negative news and reports related to criminal activities, such as human trafficking or cyber fraud, institutions can detect if individuals or organizations have been involved in activities linked to Pig Butchering scams. This proactive approach allows for better risk management and ensures that financial institutions are not unknowingly facilitating the operations of illicit networks. By integrating adverse media screening with existing AML protocols, organizations can strengthen their defenses against the financial underpinnings of these scams.

Summing Up

The Pig Butchering Scam is a cruel and sophisticated fraud that preys on trust and emotional vulnerability. By understanding the story behind this scam, recognizing its warning signs, and implementing key protective strategies, individuals can shield themselves from becoming victims.

Staying vigilant, staying informed, and keeping in mind that genuine relationships and investments are built on transparency and trust, not secrecy and pressure.

AML Watcher

About Us

At AML Watcher, we aim to support more than 10,000 businesses in their fight against rising FinCrime by creating a secure and compliant financial world where they can thrive. Supporting 10k+ business partners, Reducing $10M compliance cost, and saving 50% of screening cost.

AML Watcher maintains such features as 1300+ watchlist databases, over 200+ sanction regimes, 235+ countries while ensuring comprehensive coverage, over 5000 reputed and reliable media sources with global coverage and 80+ languages enabling multilingual reach solving issues of global coverage.

Today, AML Watcher is dedicated to assist you and your compliance team with custom AML Screening capabilities. Our real-time insights and advanced entity-matching algorithms free your searches of false matches. Get everything you need for AML Screening in one place.

Connect With Us:

For more information about AML Screening, visit:

Info@amlwatcher.com

www.amlwatcher.com