RedFlag
Accelerator

Scam or Investment Opportunity?

Hi, kindly message me on Whatsapp. I'm not always here...

Hi, Jasmine, sure, here's my whatsapp, 07795319704

Thanks really, you seems nice, i hope we can be friends

I live near Queens Park. Originally from Singapore

How about you, are you also live here?

Singapore must be nice. What brings you to London?

Thanks, i came here for work, Im working as a business analyst. How about you?

Cool, im genuinely interested in what you do. Would you like to meet..?

Investigation Guide

Pig butchering - US-Based investment scam victim

With RedFlag Accelerator, you know:

What to look for and How to find it

....Resulting in efficiently and accurately identifying customers of concern.

What is RedFlag Accelerator?

RedFlag Accelerator is an international, award-winning source of persona-based human trafficking red flags. It is a next-level, game-changing tool that brings into plain sight what is hidden in billions of lines of data in banking systems. It is developed from extensive research, data gathering, and analysis from over 350 source documents.

Table of contents

US citizens are the most targeted population

In 2023 US victims reported losses of **US $4.6 billion**

Our Approach

How to use this investigation guide

Purpose:

This is a practical, step-by-step reference guide to help you efficiently and effectively detect victims of pig butchering investment scams in your customer data.

For whom:

This is primarily aimed at financial crime investigators within financial institutions.

How to use it:

Steps 1 and 2, in the 'What to Look For' section, provide the knowledge you need to identify victims of pig butchering investment scams and describe how their financial footprint fits into the wider typology.

Having digested the knowledge, steps 3 to 6 in the 'How to find it' section help you apply it. In particular, when responding to alerts raised on individual customers, jump to steps 5 and 6.

This will help you consider the wider context of the alert and give tips on follow-up actions. When proactively considering a wider investigation across many customers, sequentially work through from step 3.

The following terminology is used throughout this guide:

Persona – a customer profile of socio-economic and financial characteristics that represent a pattern of living.

Red Flag – a behaviour or characteristic which can help identify customer instances of a given persona from their financial footprint.

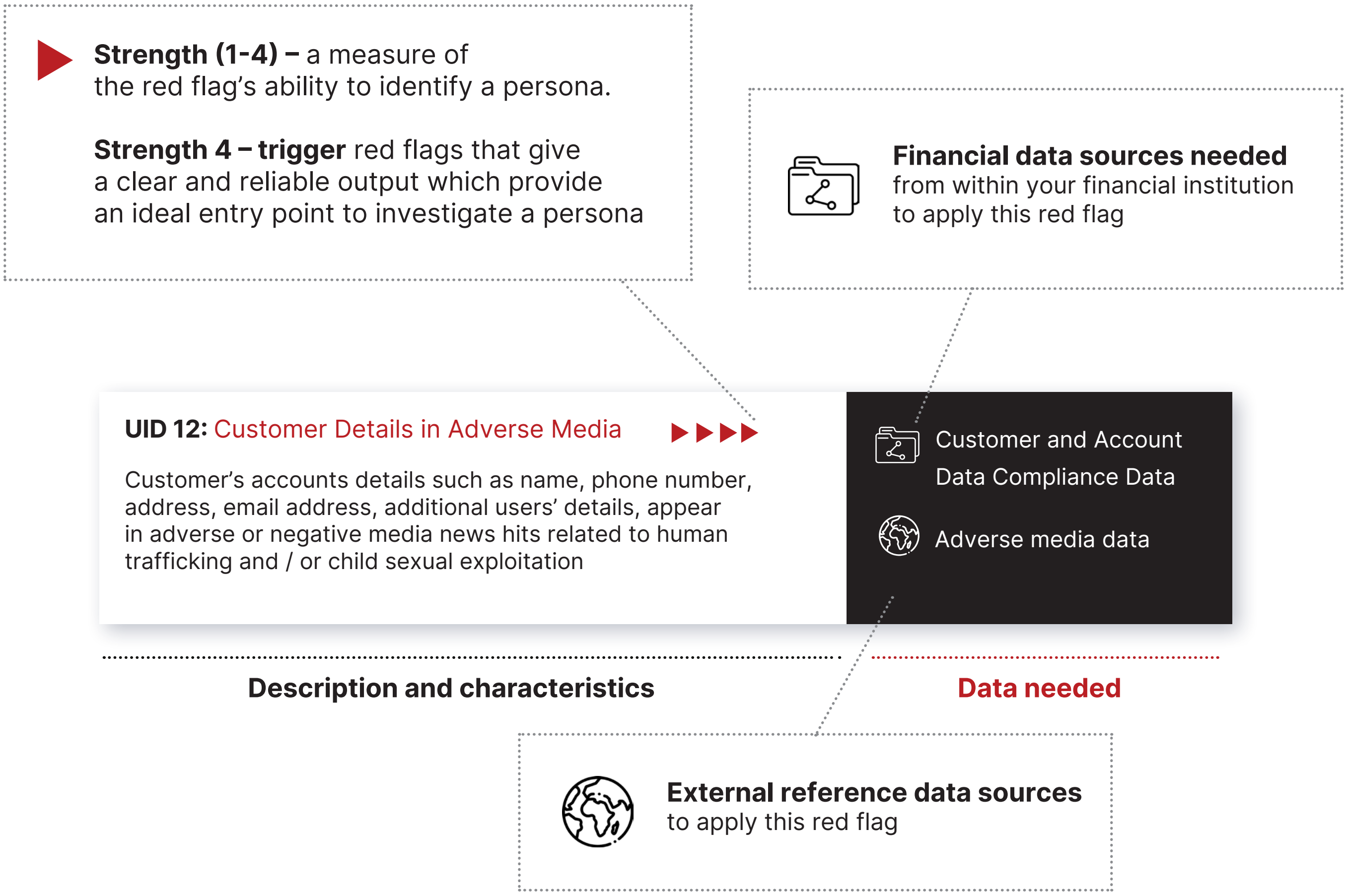
Methodology:

RedFlag Accelerator consolidates hundreds of sources of human crimes intelligence such as pig butchering into a library of contextual financial red flags and personas. All red flags are enhanced and enriched with attributes, data sources, and external reference data types required to apply them.

No one red flag occurring in isolation is sufficient to match a customer to a pig butchering persona with confidence. That’s why we group the red flags by the criminal and victim personas they represent. These personas for different types of human crimes are further grouped into typologies.

This guide focuses on victims of pig butchering investment scams and includes red flags for this persona in the ‘What to look for’ section.

Below is an example illustration showing what is included in each red flag. This covers both their characteristics and the different data types and internal and, where relevant, external data sources needed to evaluate them.



▶ **Strength (1-4) –** a measure of the red flag’s ability to identify a persona.

Strength 4 – trigger red flags that give a clear and reliable output which provide an ideal entry point to investigate a persona

Financial data sources needed from within your financial institution to apply this red flag

UID 12: Customer Details in Adverse Media ▶▶▶▶

Customer’s accounts details such as name, phone number, address, email address, additional users’ details, appear in adverse or negative media news hits related to human trafficking and / or child sexual exploitation

Customer and Account Data Compliance Data

Adverse media data

Description and characteristics

Data needed

External reference data sources to apply this red flag

What to Look For

1. Understand the typology

Link to Finance

In a digital age where personal connections often begin with a swipe or click, Shāz Hū Pán, also known as pig butchering, is a prolific financial scam blending emotional manipulation with bogus investment schemes. Predominantly orchestrated by organized crime syndicates within Southeast Asia, particularly in Special Economic Zones of Myanmar, Laos, Cambodia, and Thailand, it's a complex scheme with terrible consequences for victims across the globe.

Criminals use sophisticated tactics and specialized teams to manipulate victims through social engineering on dating apps, social media, and chat applications. They lure victims with fake high-return investments, and "train" them how to "start investing". Scammers at first mimic legitimate investment gains, urging more investment and tying it to personal bonds. When victims seek withdrawals or hesitate, they're often extorted for fees, locked out, or their accounts vanish with their investments.

Financial institutions and crypto exchanges unwittingly facilitate money laundering for criminals enabling them to move and clean funds from scams. Criminals exploit both traditional banking channels and blockchain technology, which underlies cryptocurrencies, to integrate illicit funds into the financial system.

Persona Summary

Victims of pig butchering scams often represent a cross-section of society, transcending age, educational background, and financial acumen.

Most pig butchering scams target individuals between the ages of 30 and 49 who are highly connected on social media and may have greater awareness of crypto, but recently the elderly are increasingly victims of pig butchering too.

Scammers often target vulnerable individuals who may be experiencing life-changing events, such as divorce, health issues or the loss of a loved one, making them more susceptible to the tactics of the scammer. Anyone can be a target, because all people are vulnerable in one way or another, whether it be emotionally, financially, or socially.

In 2023, US-based victims alone lost more than 4.5 billion dollars to crypto-related investment scams, with some loss estimates reaching over 75 billion dollars. The true scale of losses is unknown, because victims are often too embarrassed to report these crimes to authorities. The average loss per victim can range from a few thousand to hundreds of thousands of dollars, with some individuals losing their entire life savings.

Transactions

Abnormal transactional activity in previously dormant or low-activity bank accounts, particularly large and frequent transfers to a CEX (Crypto-exchange) or shell company with no discernible business relationship or purpose, further illustrates the depth of the victim's entanglement. Transactions are often accompanied by notes indicating payments for "taxes," "fees," "penalties," or even "AML" (Anti-Money Laundering) obligations—terms strategically employed by scammers to legitimize their demands and to manipulate victims into compliance.

The use of cryptocurrency as a preferred payment method further complicates tracking and recovery efforts, as transactions can be conducted anonymously and across international borders.

Wider context

Scammers, referring to victims as 'pigs,' carefully build trust before enticing them into a cryptocurrency investment scheme, while many scammers are victims themselves. Often scammers are young adults from various countries, lured under false pretences and then coerced into scamming and forced, forced to work under threat of violence against them or their families.

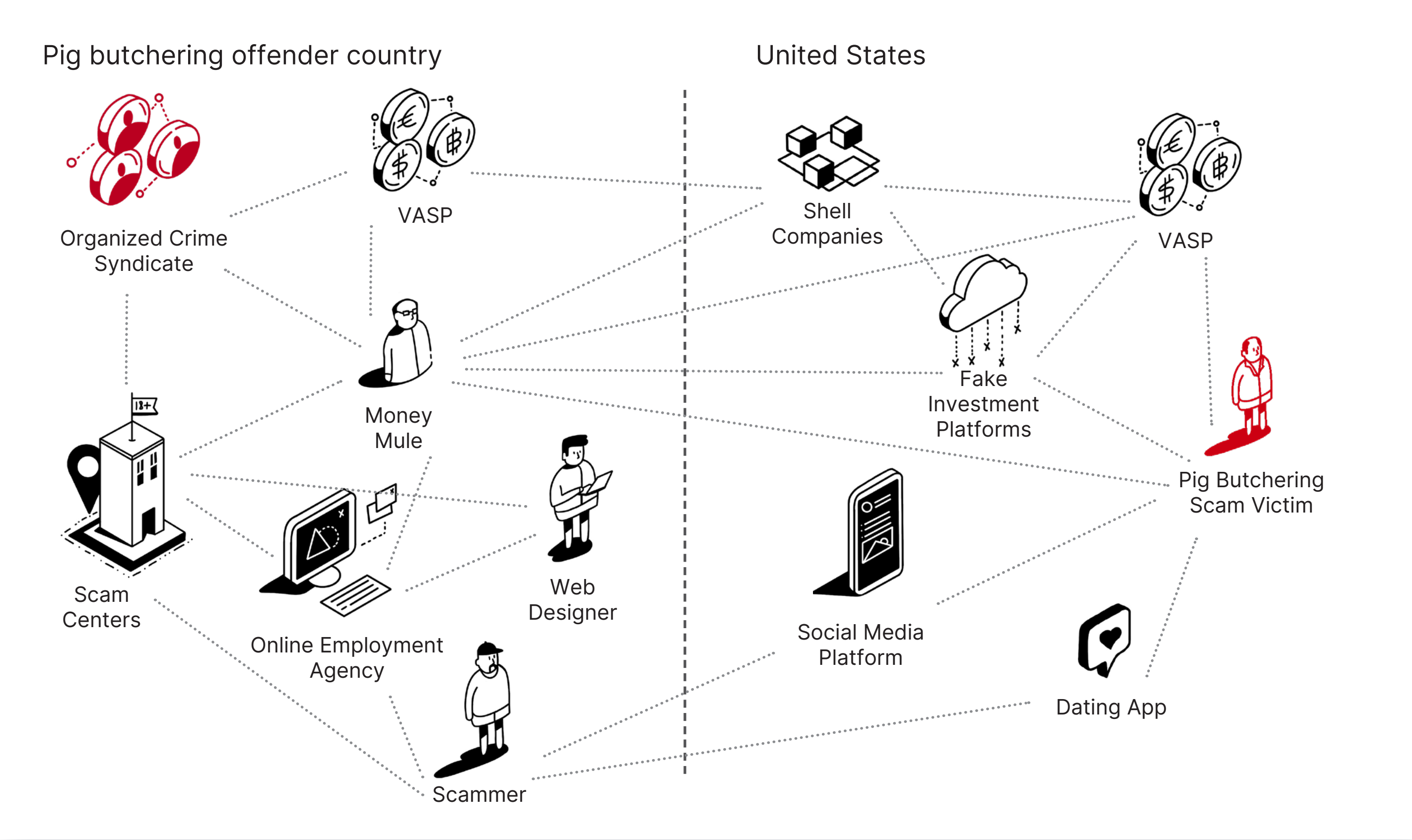
Addressing pig butchering scams demands a comprehensive strategy: enhancing financial systems' detection capabilities, bolstering prevention efforts, and prioritizing education and awareness across both private and public sectors.

PROFILE: Pig Butchering Scam Victim

- Adult, aged 30-49
- Financially Stable
- Access to Internet

This shows recurring profile characteristics evident for this persona. Customers not matching this profile may still represent the persona.

Personas network map (US)



The above persona network map shows the wider view of pig butchering investment scams, where links between these personas represent the expected flows of money.

In this network map, personas can be split between those located within the United States and those located in the region of the corresponding scam centres (often, in South-East Asia).

What to look for

2. Source red flags

UID 444: Transacting Parties in Investment Scams related Adverse Media

Customers' frequent transacting parties such as trusted creditors appear in adverse or negative media news hits related to investment scams. This may indicate a criminal network

Customer and Account Data
Compliance Data
Transaction Data

Investment Scams-related Adverse Media Data

UID 445: Transacting Parties in Investment Scams related OSINT

Customers' frequent transacting parties such as trusted creditors appear in Open Source Intelligence related to investment scams. This may indicate a criminal network

Customer and Account Data
Compliance Data
Transaction Data

Investment Scams-related OSINT Data

UID 382: Inexplicable Crypto-related Expenditure

An individual customer makes large, frequent transfers to centralized cryptocurrency exchanges (CEXs), a type of VASP, with no clear business rationale. The risk is heightened if there is:
- no previous history of such activity, as it might indicate an investment scam
- transfers are in round amounts ($1,000, $5,000, $10,000, etc.)

Transaction Data

VASP Identifiers

UID 387: Deposit Received from VASP/CEX

An individual customer's account receives a deposit from a centralized cryptocurrency exchange (CEX), a type of VASP, that is a slightly higher amount than what the customer previously transferred out to this CEX. The risk is heightened if this deposit is then followed by outgoing transfers from the customer to this CEX in substantially larger amounts

Transaction Data

VASP Identifiers

UID 380: Sudden Increase in Liquid Assets

An individual customer unexpectedly liquidates assets or takes significant financial measures, such as borrowing against savings or property (a HELOC, home equity loan, or second mortgage), to make assets available. The risk is heightened if these assets are invested in cryptocurrency, likely based on external guidance

Customer and Account Data
Transaction Data

VASP Identifiers

UID 385: Family Involvement in Crypto Expenditure ▶▶▶

An individual customer’s family members exhibit similar behavior by making large, frequent transfers to the same centralized cryptocurrency exchange (CEX) as the customer, with no clear business rationale. Or they transfer unusually high amountsof funds to the customer, which are then sent to that CEX

Customer and Account Data
Transaction Data

Parties Relationship
VASP Identifiers

UID 383: Payment References to VASPs ▶▶

A customer’s account shows unusual patterns of frequent outgoing transfers sent to one or more centralized cryptocurrency exchanges (CEX), a type of VASP, containing similar payment references such as ‘investment,’ ‘taxes,’ ‘fees,’ ‘penalties,’ mention of ‘AML requirements,’ or similar. This may indicate a common instruction given by the perpetrators of investment scams

Transaction Data

VASP Identifiers
Keywords in the Payment Reference

UID 384: Urgent Need to Access Funds ▶▶

Customer displays unusual behavior when interacting with staff at the bank branch or online and seems pressured or anxious to meet the demands or timelines for a supposed investment opportunity

Customer and Account Data
Staff Observations Data

UID 388: Inexplicable Creditors Following Crypto Activity ▶▶

An individual customer with a short history of sending several small-value transfers to a CEX/VASP abruptly stops sending funds and begins sending multiple high-value wire transfers to unrelated creditors (holding companies, limited liability corporations, individuals with no prior transaction history). This may be indicative of a victim sending trial transactions to a scammer before committing to and sending larger amounts. The risk is heightened if the creditors are located in or linked to high-risk pig butchering scams countries

Compliance Data
Transaction Data

Parties Relationship
VASP Identifiers
High-Risk Pig Butchering Scammer Countries

UID 389: Transacting with Third-party Investment Apps ▶▶

Customer mentions to bank staff that they downloaded an application to make crypto-related investments on their phone directly from a third-party website, rather than from a well-known application store

Customer and Account Data
Staff Observations Data

UID 51: Change in Cash Withdrawal Pattern ▶▶

Customer's accounts show a sudden change in cash withdrawal behaviour when compared to the historic averages and patterns with no apparent reason. This includes a sudden increase in the frequency, aggregate amount and/or location

Transaction Data

UID 392: Customer Activity at Bitcoin ATM ▶▶

Customer's bank card statement shows patterns of transactions for large round dollar amounts at Bitcoin ATMs. This may indicate a crypto-related scam where offender is instructing customer to deposit funds through Bitcoin ATM

Customer and Account Data
Transaction Data

Bitcoin ATM Operators

UID 386: Poor Reputation VASPs/CEXs ▶

A customer's account shows unusual patterns of frequent outgoing transfers sent to one or more centralized cryptocurrency exchanges (CEX) or other VASPs which are known for their poor reputation. These CEXs/VASPs tend to have a very limited digital footprint, no social media presence or low download numbers, or have been reported for not meeting regulatory standards, which could indicate a lack of legitimacy

Transaction Data

VASP Identifiers
Poor Reputation VASPs/
CEXs

UID 381: Sudden Non-sufficient Funds Activity ▶

An individual customer with a stable account balance history suddenly starts incurring non-sufficient funds (NSF) activity and related charges or shows a low account balance

Customer and Account Data
Transaction Data

How to find it

Include steps 3 and 4 when assessing the risk of the pig butchering scam personas being present throughout your customers data. For individual customer's alert, skip to step 5 (page 9).

3. Make it relevant

Use the 'data needed' part of the red flags in the previous section to identify the flags where you can access reliable data.

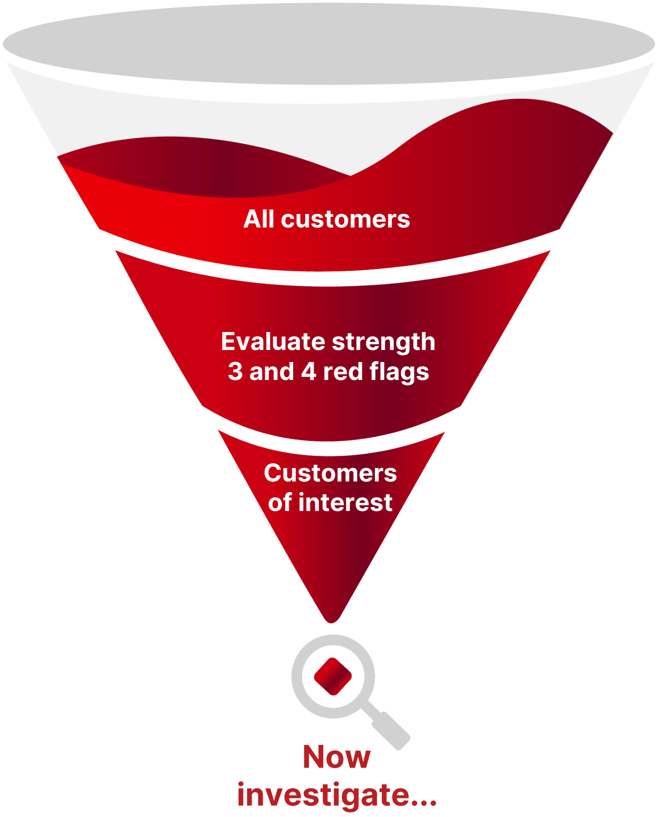
Gather the necessary external reference data to evaluate the red flags.

4. Reduce the noise

Trigger red flags which have the highest strength should be evaluated for all customers.

Filter customers to select only those for which one of these trigger red flags is activated.

Now you are ready to investigate these customers in step 5.



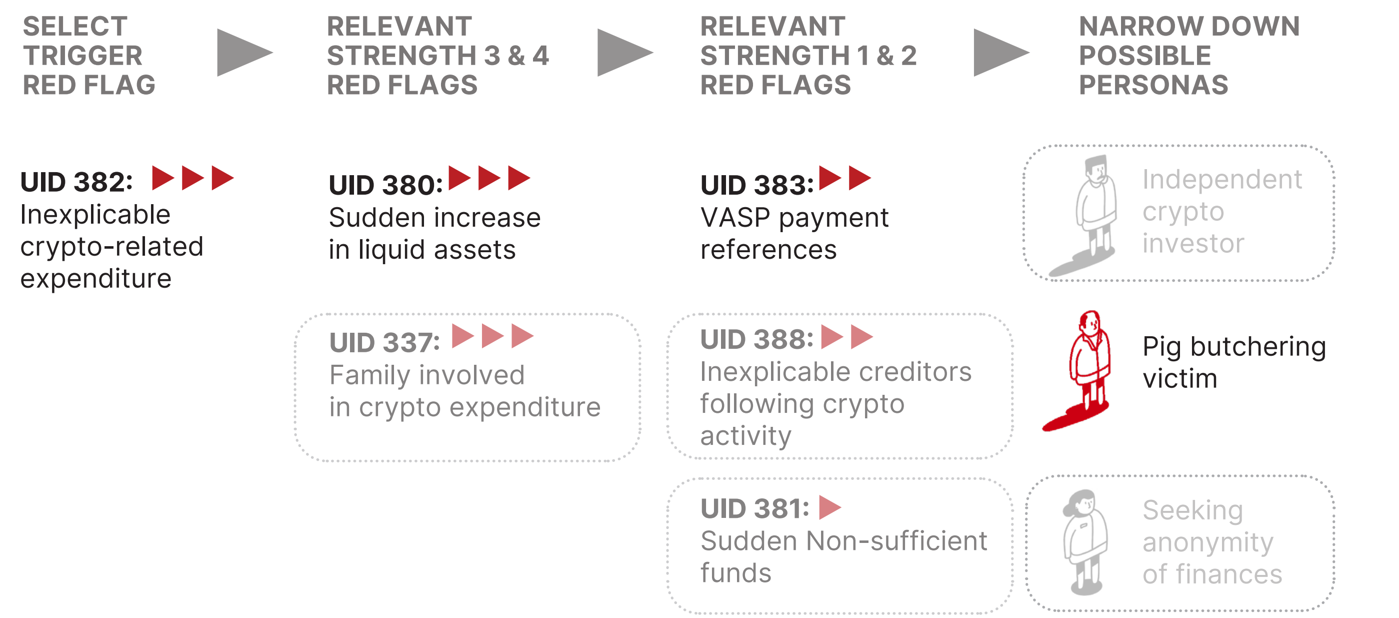
How to find it

This step helps you investigate customers for whom an initial concern has been raised. This may be following step 4 or another trigger such as those below.

5. Investigation steps

- Consider the possible criminal, victim and legitimate personas for the behavior which has triggered the concern. The persona network map in the ‘Understand the typology’ section may help.
- For each identified possible persona, consider their likely profile characteristics and use the red flags from step 2 that best distinguish the target victim of pig butchering investment scams from the other possible personas. Focus on red flags for which the ‘data needed’ is easily accessible.
- Of the identified red flags, first evaluate those of higher strength and only progress to lower strength red flags if these point to high-risk personas.

Example Investigation Pathways



SELECT TRIGGER RED FLAG ▶ RELEVANT STRENGTH 3 & 4 RED FLAGS ▶ RELEVANT STRENGTH 1 & 2 RED FLAGS ▶ NARROW DOWN POSSIBLE PERSONAS

UID 382: ▶▶▶ Inexplicable crypto-related expenditure

UID 380: ▶▶▶ Sudden increase in liquid assets

UID 337: ▶▶▶ Family involved in crypto expenditure

UID 383: ▶▶ VASP payment references

UID 388: ▶▶ Inexplicable creditors following crypto activity

UID 381: ▶ Sudden Non-sufficient funds

Independent crypto investor

Pig butchering victim

Seeking anonymity of finances

Investigation steps above illustrate an example where a TMS system has flagged a customer for transferring a total of $60,000 to a CEX over 5 transactions within the last month.

- Three possible personas are identified as explaining the TMS system trigger.
- Using the 'Source red flags’ section of this guide and availability of data needed, two other strength 3 and 4 red flags are identified as helping differentiate the target persona from the other two possible personas. Additionally, three relevant strength 1 and 2 red flags are similarly identified and assessed.
- The results point to the pig butchering scam victim being the most likely persona, so we proceed to step 6.

How to find it

This step gives tips on how to proceed with customers which are likely to represent identified criminal or victim personas for which further action is required.

6. Next steps

Having matched a customer to being a potential victim of pig butchering, before raising a SAR it may be helpful to do additional checks to collect more details. Checking for the presence of any additional red flags for the persona listed in Step 2's 'Source the Red Flags' section may help add additional relevant context.

High quality, accurate and timely SAR's can help stop investment scams such as 'pig butchering'. When raising a SAR, include all relevant supporting information for the identified red flags. In particular, FinCEN advise to:

Take care in completing the narrative section of the report to provide a clear complete and concise description of the possible criminal activity.

Include any relevant technical cyber indicators related to cyber events and associated transactions within the available structured cyber event indicator fields on the SAR form or as part of the attachment field.

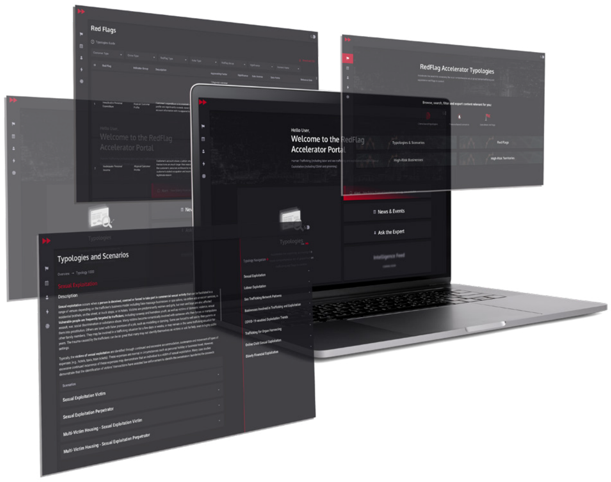
IN SAR Field 2, include 'FIN-2023-PIGBUTCHERING' and reference the code in the narrative.

Select "Fraud-Other" under SAR field 34(z) with the description pig butchering.

If applicable, when filing a Form 8300, select Box 1b ("suspicious transaction") and include the key term "FIN2023-PIGBUTCHERING" in the "Comments" section of the report.

Additionally, financial institutions are encouraged to refer their customers who may be victims of pig butchering to the FBI's IC3: https://www.ic3.gov/. Financial institutions may also refer their customers to the Securities and Exchange Commission's tips, complaints, and referrals (TCR) system to report investment fraud: https://www.sec.gov/tcr.

In the case of elder victims of pig butchering, banks may refer their customers to DOJ's National Elder Fraud Hotline at 833-FRAUD-11 or 833-372-8311.

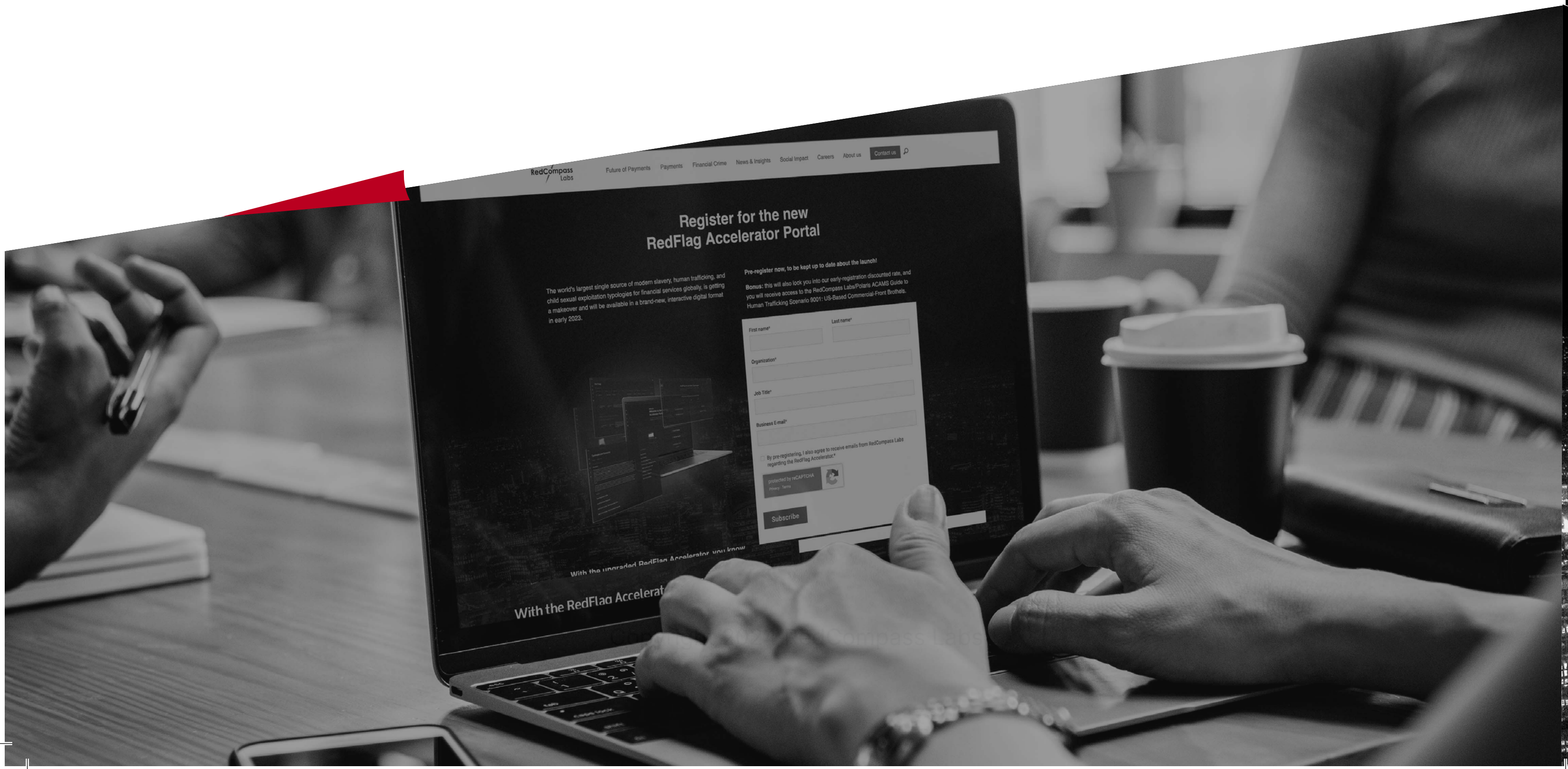

Red Flags
RedFlag Accelerator Typologies
Welcome to the RedFlag Accelerator Portal
Typologies and Scenarios
News & Events
Ask the Expert

To fight human trafficking in financial data, you need to know what to look for, and how to find it. With RedFlag Accelerator, you can.

Contact us to learn about Investigation and Detection Packs including:

- Exclusive Portal Access
- External Reference Data from trusted sources
- Scientific Anti-bias Risk Scoring Algorithms
- Advanced AI Data Analytics

- Seamless Integration via ready-to-use Microservices
- Industry-leading Professional Services, to support on:
  - Knowledge transfer and training
  - Technical integration
  - Data science



Register for the new RedFlag Accelerator Portal

The world's largest single source of modern slavery, human trafficking, and child sexual exploitation typologies for financial services globally, is getting a makeover and will be available in a brand-new, interactive digital format in early 2023.

Pre-register now, to be kept up to date about the launch!

Bonus: this will also lock you into our early-registration discounted rate, and you will receive access to the RedCompass Labs/Polaris ACAMS Guide to Human Trafficking Scenario 9001: US-Based Commercial-Front Brothels.

First name*

Last name*

Organization*

Job Title*

Business E-mail*

□ By pre-registering, I also agree to receive emails from RedCompass Labs regarding the RedFlag Accelerator.*

protected by reCAPTCHA
Privacy - Terms

With the upgraded RedFlag Accelerator, you know

With the RedFlag Accelerat

Learn more

REGISTER FOR THE NEW
REDFLAG ACCELERATOR PORTAL

RedFlag Accelerator

WWW. REDFLAGACCELERATOR.COM