RedFlag Accelerator

Real Person or Extortionist?

Investigation Guide

US-Based financial sextortion victim

With RedFlag Accelerator, you know:

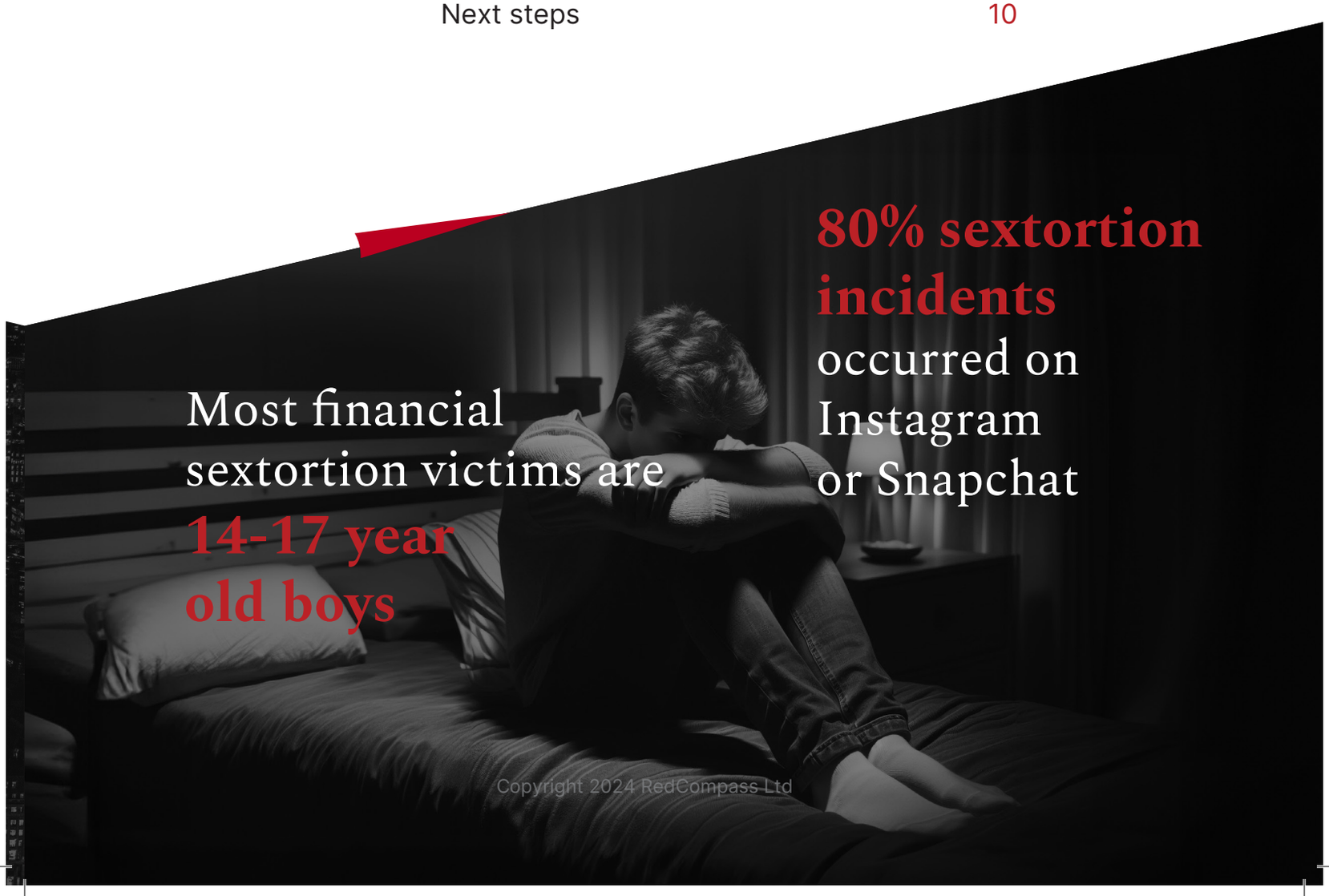
What to look for and How to find it

....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



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 financial sextortion victims 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 financial sextortion victims 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.

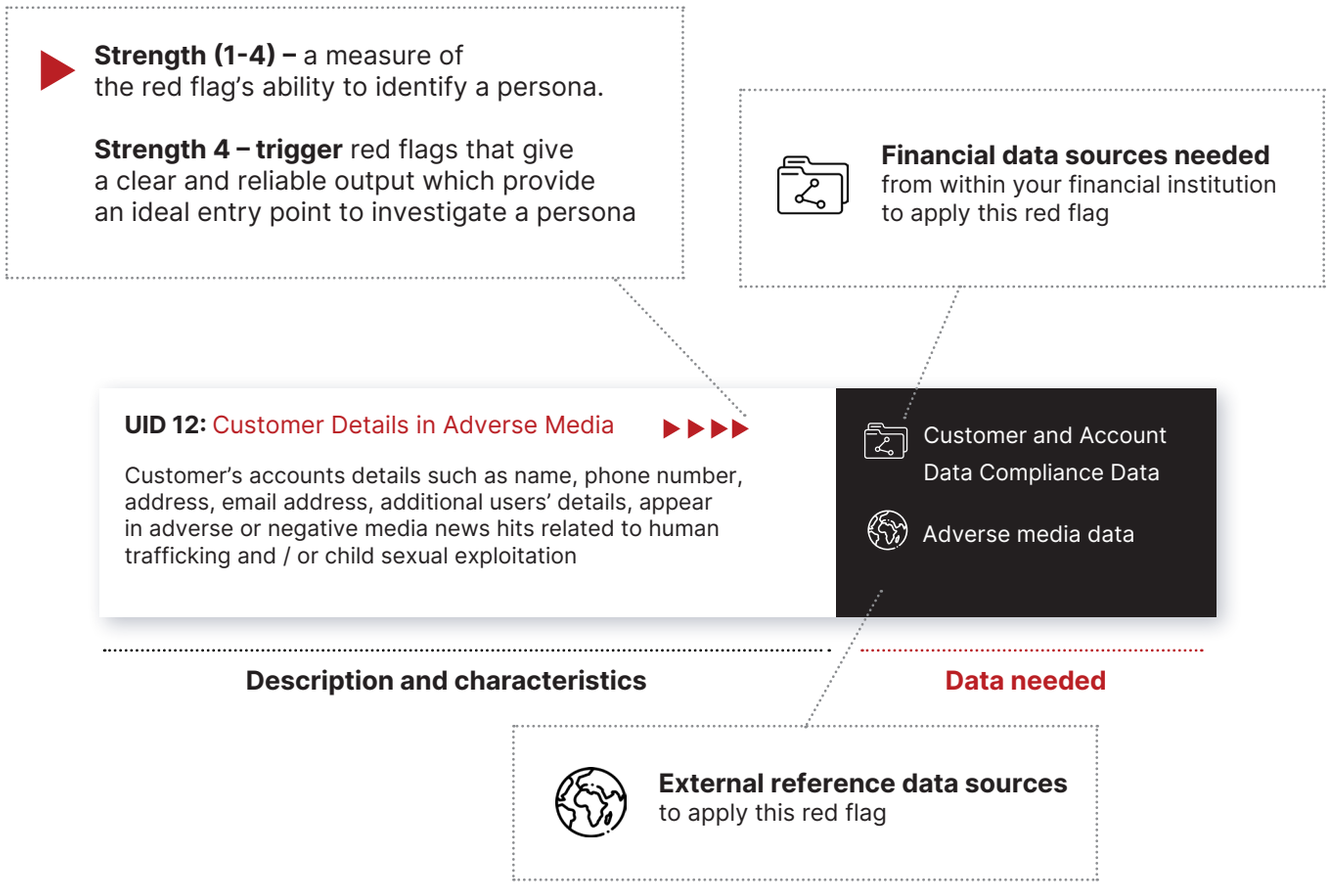
Methodology:

RedFlag Accelerator consolidates hundreds of sources of human crimes intelligence such as financial sextortion 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 sextortion 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 sextortion victims 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.



What to Look For

1. Understand the typology

Link to Finance

Financial sextortion is the fastest growing crime targeting children and young men in North America. Criminals pose as someone else online to coerce victims into sharing sexually explicit images, and then immediately demand payment or threaten to release the images to the victims' family and friends.

The tactics of coercion employed by online offenders can inflict substantial fear and psychological harm on the victims, sometimes leading to tragic outcomes.

The financial aspect of sextortion involves payments made by victims to offenders to comply with extortion demands and prevent the release of explicit material. Signs of sextortion in victims' financial behavior include sudden or unexplained changes in their financial activities. Recognizing these patterns can aid financial institutions in detecting and disrupting these illicit activities.

Persona Summary

Over 90% of financial sextortion victims in the United States are males, with the most targeted group being those aged 14 to 17 who have access to the internet and smartphones. They are approached and coerced into sharing sexually explicit images through online platforms such as social media, dating apps, and online gaming.

These young individuals often lack financial resources and may resort to desperate measures such as theft, taking out loans, or selling their belongings. Even after complying with the offender's demands, victims may continue to face threats and extortion for more money.

It's essential for financial institutions to closely monitor the financial activities of these vulnerable individuals and recognize the tell-tale signs of sextortion that are inconsistent with typical behavior patterns for their age group.

Transactions

Financial transactions play a critical role, with victims often coerced into making payments to offenders to prevent the dissemination of explicit material. These transactions can range in size and frequency, from small, one-time payments to larger sums over extended periods. Payments can be irregular, as minors typically need time to secure funds and a payment method.

Victims usually pay between $100 and $5,000 in total before running out of funds, although some have paid up to $15,000 through various payment methods, including cryptocurrency, online peer-to-peer (P2P) payment platforms, MSBs, or gift cards.

In certain cases where victims are incapable of making payments, they may be coerced into becoming money mules. In this scenario, they are instructed to open bank accounts which are then utilized by criminals to launder illicit funds.

Wider context

The majority of recent financial sextortion schemes targeting young people in the United States for financial gain are directly linked to cybercriminal groups located in West Africa (e.g., Yahoo Boys) and other high-risk regions. A list of high-risk sextortion offender countries can be accessed in the RedFlag Accelerator Portal.

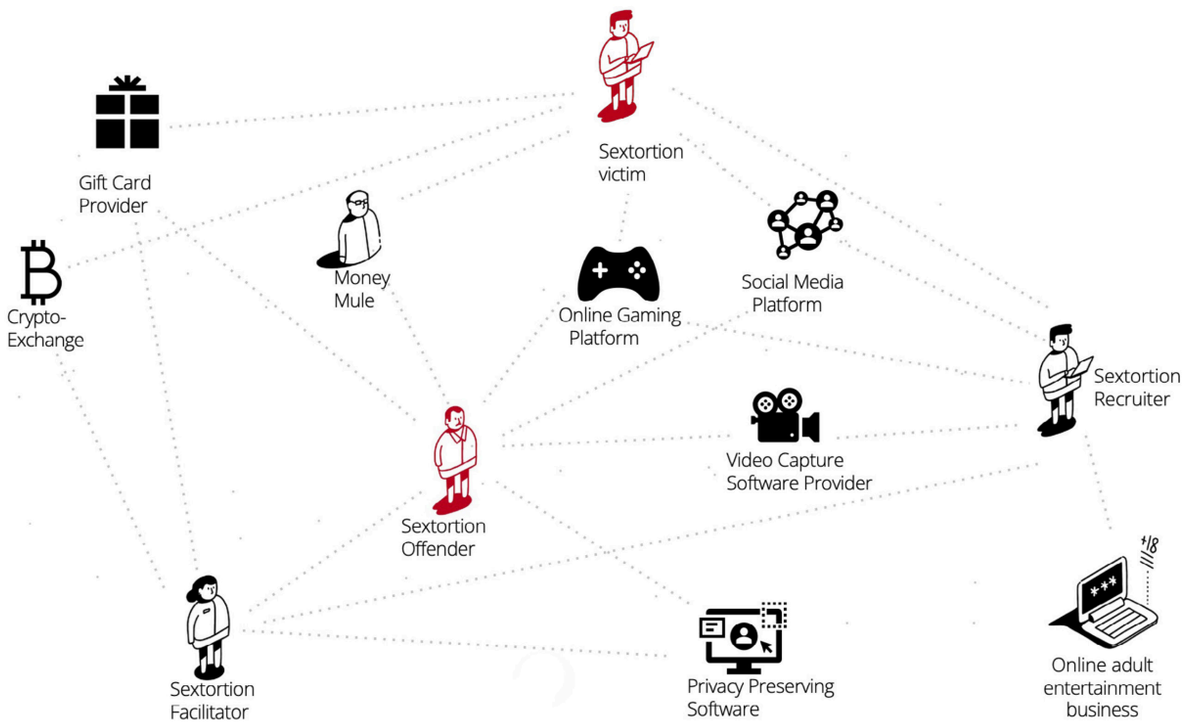
The tenfold increase in sextortion cases in the past 18 months is a direct result of these cybercriminal groups distributing sextortion instructional videos and scripts on TikTok, Instagram, and Scribd. This enables other criminals to engage in financial sextortion at scale.

PROFILE: Sextortion Victim

- Male
- Aged 14-17
- Access to Internet
- Access to Smart Phone

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

Personas network map



The above persona network map shows the wider view of the sextortion business model, where links between these personas represent the expected flows of money.

Sextortion is a global crime with offenders, recruiters and facilitators from around the world targeting victims in the US.

What to look for

2. Source red flags

UID 422: Transacting Parties in Sextortion-related Adverse Media

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

- Customer and Account Data
  Transaction Data
- Sextortion Adverse Media Data

UID 423: Transacting Parties in Sextortion-related OSINTin Sextortion-related Adverse Media

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

- Customer and Account Data
  Transaction Data
- Sextortion OSINT Data

UID 374: Sending Sextortion-related Payment References

Minor customer is sending suspicious payment references that may be related to sextortion. This may include references to any of the following:

- sexual commentary
- threatening or pleading language
- social media usernames
- references to explicit material taken including photos and videos
- social media site titles with reference to where the content is situated
- offender's name or online nickname
- time or date CSE material occurred or was requested

- Compliance Data
  Customer and Account Data
  Transaction Data
- Sextortion Payment References

UID 212: Minor Sending Funds to Inexplicable Creditor

Minor customer's accounts show patterns of payments ($100 to $2,000) sent to an unrelated individual with no apparent legitimate reason. The risk is heightened if the creditor is located in or linked to a high-risk sextortion offender country

Compliance Data
Customer and Account Data
Transaction Data

High-risk Sextortion Offender Countries

UID 362: Minor Purchasing Gift Cards

Minor customer's accounts show purchases of gift cards (such as iTunes, Steam, Roblox and others) and prepaid cards with no logical reason. In some cases offenders require this payment method, and instructs a victim to take a photo of the card and send the image as a payment

Compliance Data
Transaction Data

Gift Card Providers

UID 391: Minor Customer P2P Payments Activity

Minor customer's accounts show patterns of payments ($100 to $2,000) made to P2P payment platforms such as PayPal, CashApp, Venmo, Zelle and others. In some cases sextortion offenders instruct victims to use this payment method

Compliance Data
Transaction Data

P2P Payment Platforms

UID 390: Minor Customer Activity at Bitcoin ATM

Minor customer's bank card statement shows patterns of transactions ($100 to $4,000) at Bitcoin ATMs. In some cases sextortion offenders instruct victims to use this deposit method, and often these instructions are given in real time

Customer and Account Data
Compliance Data
Transaction Data

Bitcoin ATM Operators

UID 361: Minor Making Payments at Bank Branch

Minor attends a bank branch in person to make a payment ($100 to $2,000) to an unrelated individual to not alert their parents at home. Typically these are domestic payments to a US-based offender or a money mule

Compliance Data
Customer and Account Data
Transaction Data

UID 213: Minor Customer Activity Related to Cryptocurrency

Minor customer's accounts show transactional activity related to virtual assets (e.g., cryptocurrency):

- purchasing virtual currency (via debit or credit card, bank account, ApplePay, Paypal etc.) from virtual currency service providers (VASPs) not requiring age or ID verification such as Bybit, MEXC Global, Weex, KuCoin, Margex, PrimeXBT, and Bisq
- withdrawals from virtual currency exchanges or wallets into fiat currency (via debit or credit card, bank account etc)
- activity on P2P exchanges and mixers (e.g., Paxful, CardCash, CoinCola etc.) to exchange virtual currency from and into other means such as gift cards or third party payments, digital wallets such as Skrill

Customer and Account Data
Compliance Data
Transaction Data

VASPs with no KYC
VASP Poor Risk Rating
VASP Identifiers

How to find it

Include steps 3 and 4 when assessing the risk of the sextortion personas being present throughout your customers data. For individual customer's alert, skip to step 5 (page 7).

3. Make it relevant

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

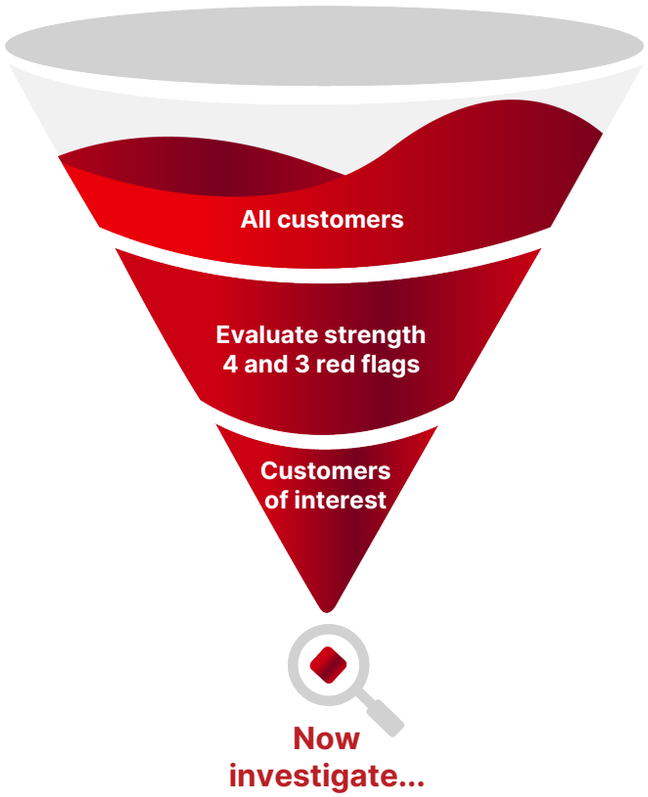
Gather the necessary external reference data to evaluate the red flags.

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.



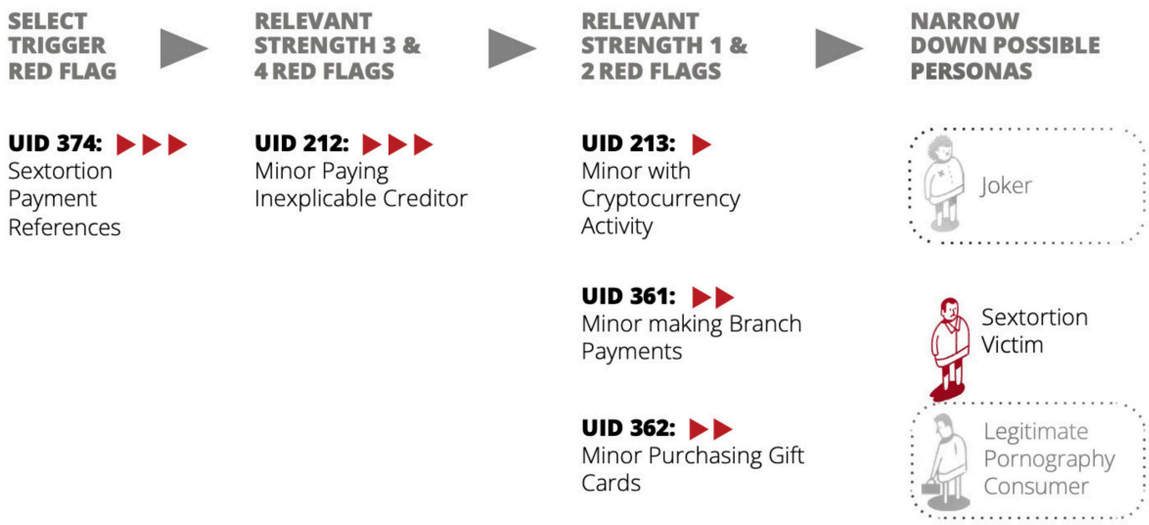
How to find it

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 behaviour 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 sextortion victim 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



Investigation steps above illustrate an example where a TMS system has flagged a minor customer for sending a $500 payment with reference 'nude pics'

- 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, one other strength 3 red flag is 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 sextortion 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 sextortion victim, before raising a SAR it may be helpful to do additional checks to collect more details both internally (e.g., cyber footprint), and externally (e.g., social media or other online presence). 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.

When raising a SAR relating to financial sextortion, FinCEN advise:

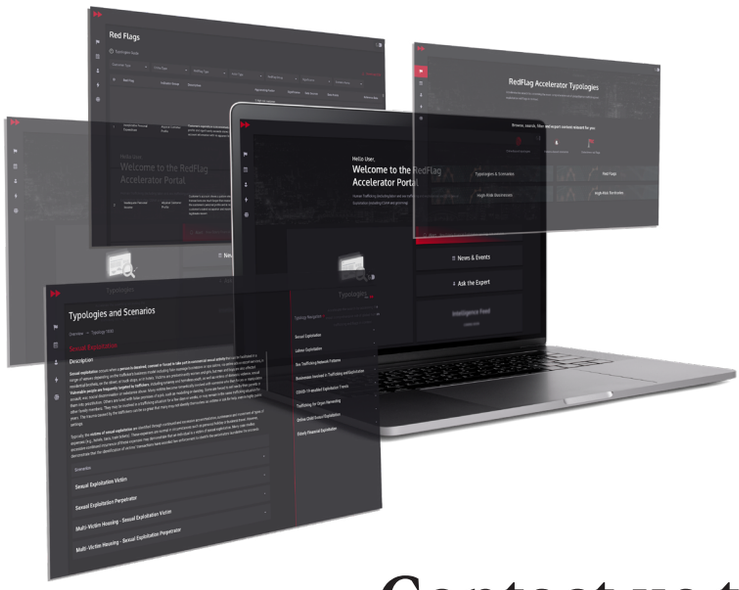
- In SAR Field 2, include 'OCSE-FIN-2021-NTC3' and reference the code within the narrative.
- Select SAR Field 38(z) (Other) and include financial sextortion in the text box.

- Use the terms and definitions in the appendix when describing suspicious activity, which will assist FinCEN's analysis.
- In SAR Field 34 include any known relevant IP addresses and dates.

- Include in the narrative chat logs, IP addresses, email addresses and filenames.
- If the SAR relates to cyber events please refer to FinCEN's FAQ guidance on additional relevant information to include.

If you have immediate information to share with law enforcement, get in touch with the National Center for Missing and Exploited Children at the Cyber Tip hotline at 1-800-843-5678.

The hotline partners with the FBI, DHS and other LEAs.

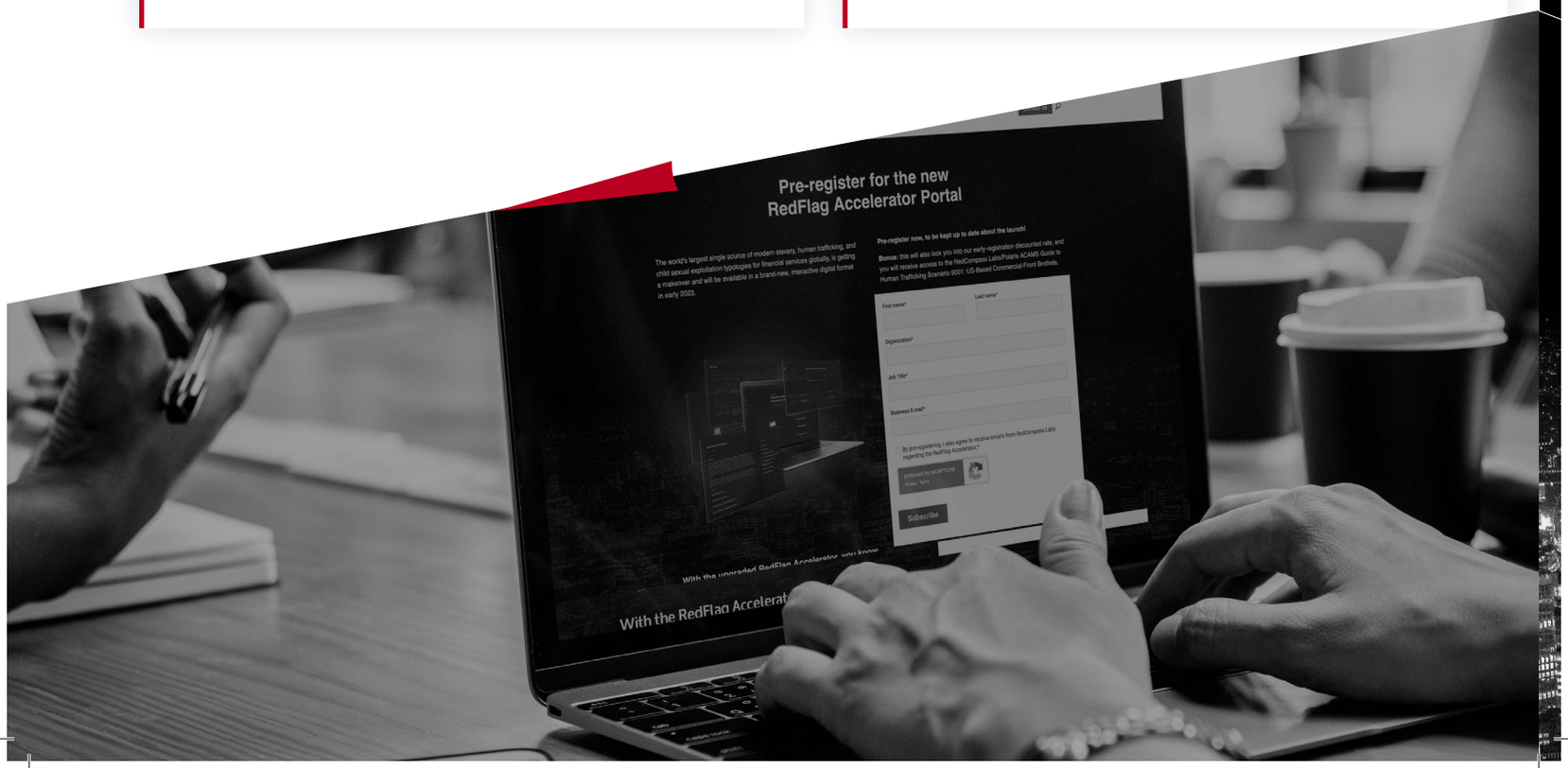


To fight human trafficking in financial data, you need to know what to look for, and how to find it. With RedFlag Accelerator, you can.

Contact us to learn about Investigation and Detection Packs including:

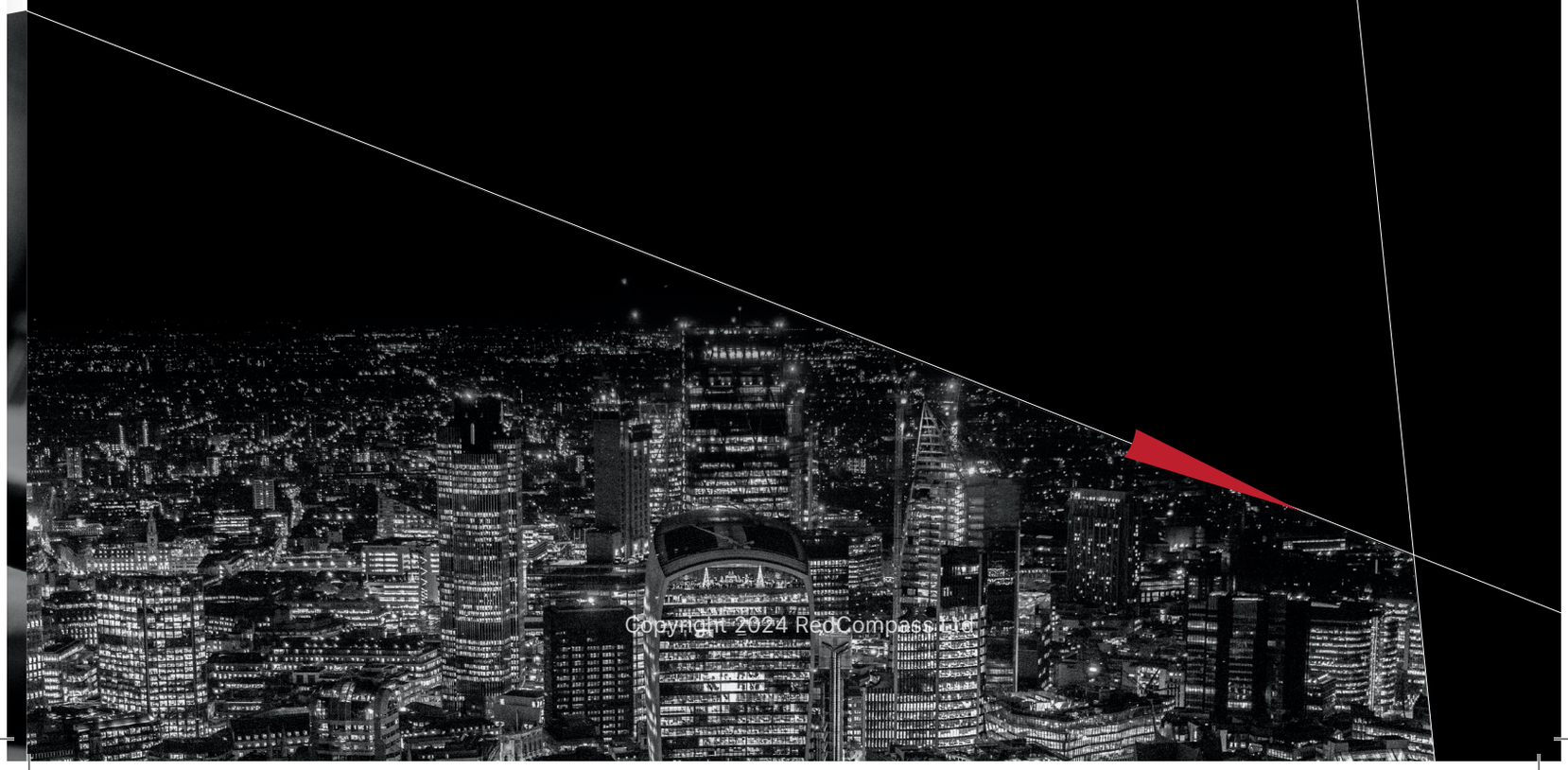
- Exclusive Portal Access
- External Reference Data from trusted sources
- Scientific Anti-bias Risk Scoring Algorithms
- Advanced AI Data Analytics

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



Learn more

REGISTER FOR THE NEW
REDFLAG ACCELERATOR PORTAL



RedFlag
Accelerator

WWW. REDFLAGACCELERATOR.COM