

Carer or Scammer?

Investigation Guide

US-Based elderly financial exploitation victim
(by unknown party)

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

How to use this guide 01

What to look for:

Understand the typology 02

Source red flags 05

How to find it:

Make it relevant 08

Reduce the noise 08

Investigation steps 09

Next steps 10



**Up to 5 million older
Americans exploited
each year**

Annual loss by victims
of financial elder abuse is
at least \$36 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 elderly financial exploitation by an unknown party 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 elder financial abuse 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:

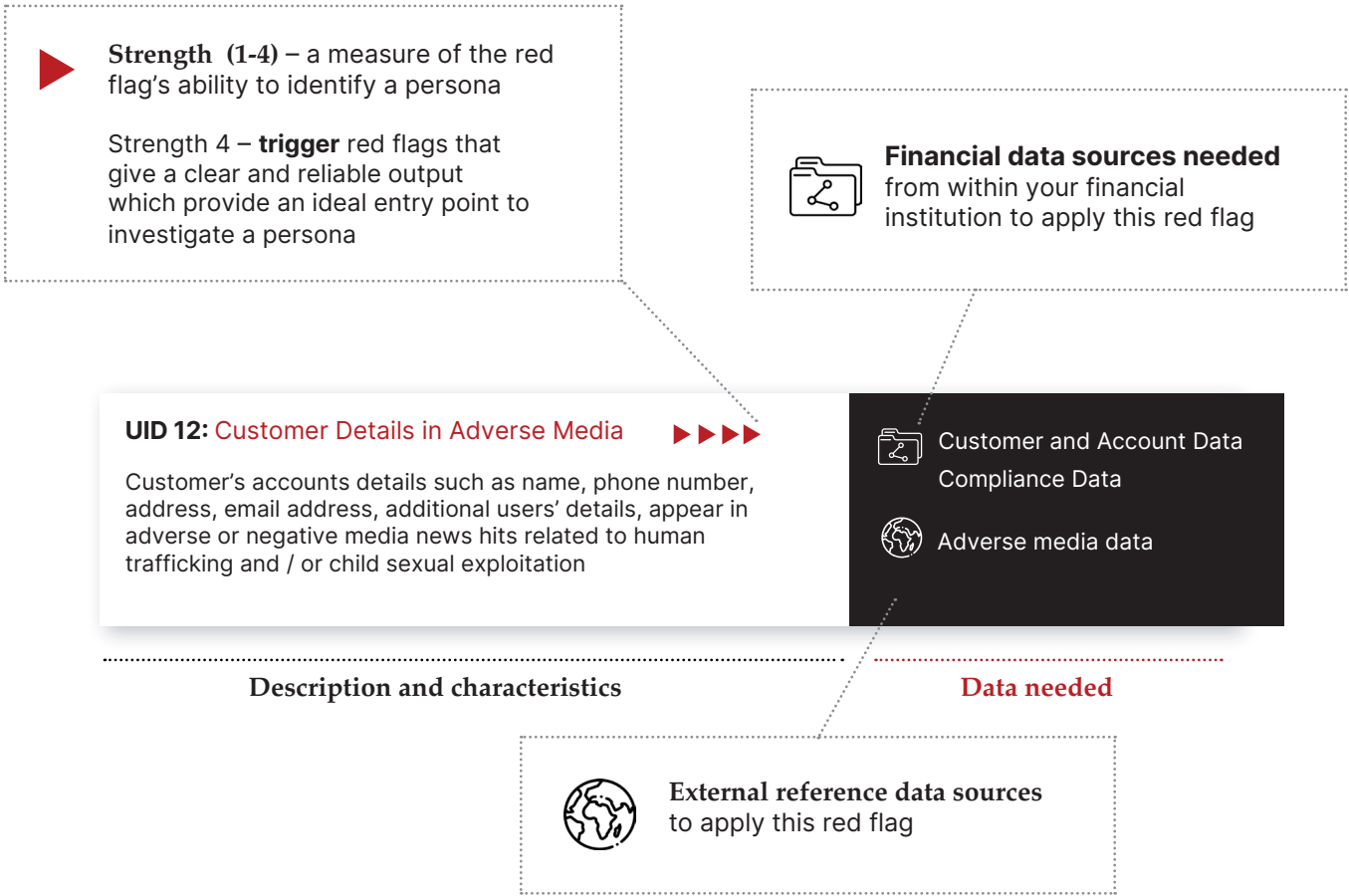
RedFlag Accelerator consolidates hundreds of sources of human crimes intelligence such as elderly financial exploitation into a library of contextual financial red flags and personas. All red flags are enhanced and enriched with attributes, data sources, and external reference data types required to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

No one red flag occurring in isolation is sufficient to match a customer to an elderly financial exploitation 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 elderly financial exploitation by an unknown party 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.

Illustrative key of red flag properties:



What to Look For

1. Understand the typology

Link to Finance

Elder financial abuse encompasses a range of financial activities targeting vulnerable seniors, serving as the conduit for exploitation.

Romance scams often involve victims wiring funds to overseas accounts under the guise of covering travel expenses or resolving fabricated financial crises. Whereas emergency/person-in-need scams exploit familial bonds, coercing elders into sending money urgently for fictitious medical emergencies or legal troubles.

Similarly, lottery scams capitalize on the victim's hopes of a windfall, prompting repeated transfers to cover fake taxes or administrative fees. Gift cards emerge as a favoured payment method due to their accessibility and lack of stringent oversight, facilitating quick cash access for scammers.

Persona Summary

Elderly people frequently fall prey to exploitation by strangers, who target them as they seem more trusting, naive, lonely, or easily confused and are likely to believe the 'pitch' of the con artist. As such, a relatively easy access to their savings has made elderly people particularly interesting for scammers.

There is no exception, people of all backgrounds may become a victim of a scam. However, the ones who have been swindled once, pose a greater risk of being scammed again. Scammers keep track of those who have fallen for a scam and sometimes distribute lists of potential leads to other con artists. As such, it is common for some seniors to be victimized multiple times.

Transactions

Most scams involve sending money abroad to a beneficiary, whom an elder has no relationship with. Victims have been known to send money in amounts ranging from \$500 to \$500,000 aggregated over time. Money Service Businesses (MSBs) are most often used to transfer the proceeds of the elderly scams. Thanks to MSBs operational model, scammers can immediately withdraw profit in cash, which prevents victims from recalling the funds, after the scam is recognized. Many con artists operate or conduct money-receiving procedures in African and Asian countries.

Gift card payments are popular amongst different types of scams, as they are easy to find and buy at big retail stores, as well as having fewer protections. Once the victim is persuaded to make an immediate payment and reveals the gift card details, money is immediately checked, often from an overseas location, and the victim has little to no chance to get it back.

Wider context

The issue of elder financial abuse extends beyond individual scams, reflecting broader societal challenges and vulnerabilities. Advancements in technology have facilitated the proliferation of sophisticated scams, making it easier for perpetrators to exploit seniors remotely and anonymously.

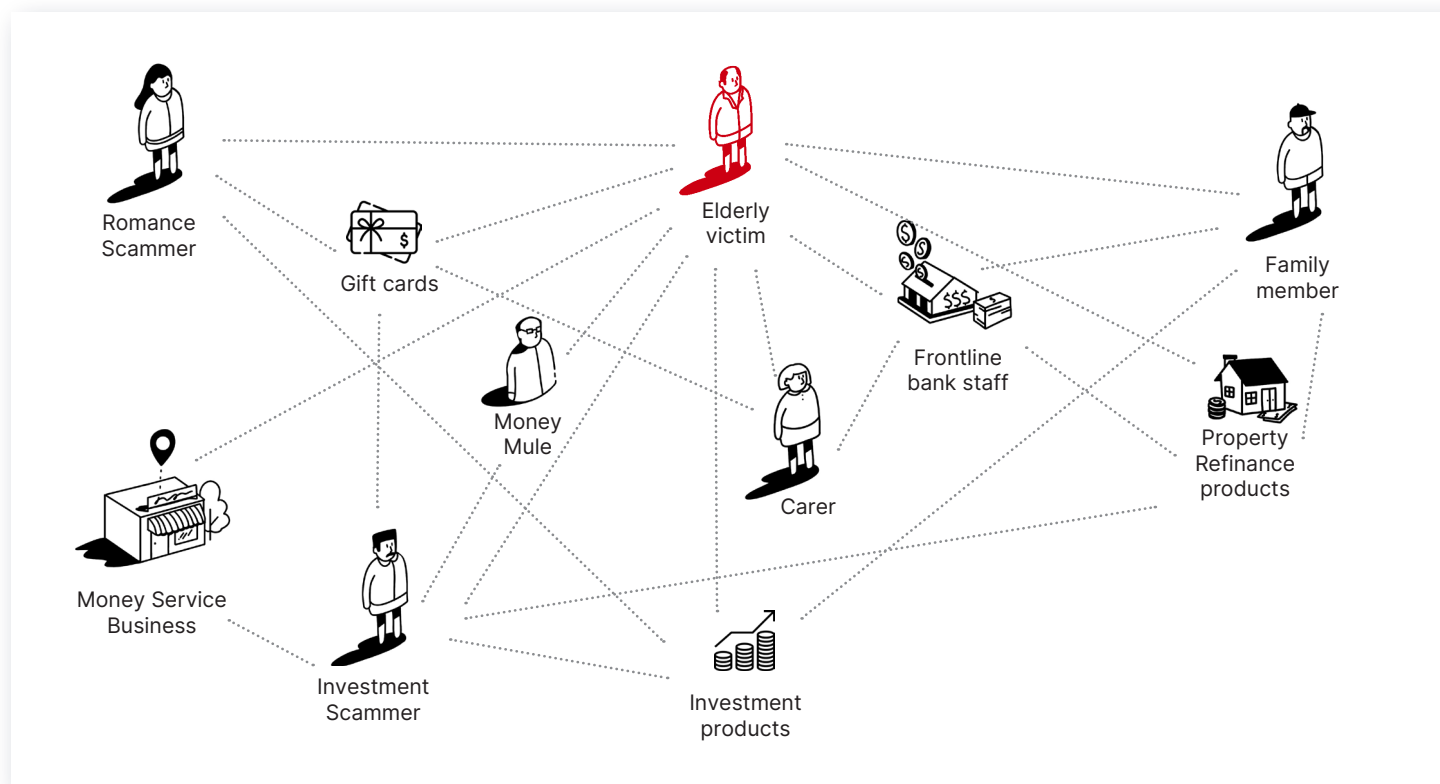
Legislative frameworks and regulatory measures play a crucial role in addressing elder financial abuse, yet gaps in enforcement and coordination remain prevalent. Collaborative efforts among government agencies, financial institutions, law enforcement, and advocacy groups are essential for combating elder financial exploitation effectively and ensuring the protection and dignity of seniors in society.

PROFILE: Elder Abuse Victim

- Pensioner
- Cognitive decline
- Dependent on others
- Lonely

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

Personas network map



The above persona network map shows the wider view of elderly financial exploitation, where links between these personas represent the expected flows of money.

Elder financial abuse by those known to the victim is typically domestic but elder abuse by remote scammers can often involve overseas perpetrators often in African and Asian countries.

What to Look For

2. Source red flags

UID 465: Transacting Parties in Elder Exploitation-related Adverse Media



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



Customer and Account Data
Compliance Data
Transaction Data



Elder Exploitation Adverse
Media Data

UID 466: Transacting Parties in Elder Exploitation-related OSINT



Customers' frequent transacting parties such as trusted creditors appear in open source intelligence leads related to elder exploitation and/or more generalized investment scams. This may indicate a criminal network



Customer and Account Data
Compliance Data
Transaction Data



Elder Exploitation Adverse
OSINT Data

UID 328: Significant Cash Withdrawals from Senior's Account



Sudden changes in accounts or practices, such as unexplained withdrawals of large sums of money, particularly when a vulnerable customer is escorted by another person (e.g., caregiver, family member, 'friend') who appears to be directing the changing activity patterns



Customer and Account Data
Transaction Data

UID 329: Frequent ATM Cash Withdrawals from Senior's Account



Frequent large withdrawals at the ATM, often to the daily maximum limit. Especially if the card has been recently issued or are used shortly after the addition of a new authorised users, or addition of a new power of attorney



Customer and Account Data
Compliance Data
Transaction Data

UID 331: Senior Making Large Transfers



Sudden changes in a senior's banking behaviour, such as uncharacteristic attempts to wire large sums of money, especially if creditor is located abroad (Africa, Asia)



Transaction Data

UID 334: Savings Suddenly Withdrawn

Customer's account shows large transfers into the account from investment accounts, without regard to pre-mature closure penalties, only to be quickly withdrawn



Transaction Data

UID 336: Senior's Activity Related to Gift Cards

Senior purchases gift card at one or multiple retail stores (not to raise cashier's suspicion) or makes a round amount payment to online gift card suppliers. Victims of gift cards scam are often directed to large retailers (Walmart, Target, CVS or Walgreens) to purchase gift cards or requested to put money on eBay, Google Play, Target or iTunes card and then asked to reveal the numbers on the back of the card. It can be used online or in store to buy items that can then be sold for profit. Such behaviour is particularly suspicious when gift card values are immediately checked from overseas locations

Customer and Account Data
Transaction Data

Gift Card Providers

UID 337: Sudden Changes in Appointed Fiduciaries

Customer's profile shows abrupt changes to financial documents such as power of attorney, account beneficiaries, wills and trusts, property titles, deeds and other ownership documents, particularly if the changes are unexpected, sudden, or favour new acquaintances

Customer and Account Data
Compliance Data
Transaction Data**UID 341: Senior's 'New Friend' Appearance**

A sudden appearance of a new caretaker, or friend who conducts financial activity on behalf of a senior without proper documentation. Customer abruptly moves away from existing relationships and toward new associations with other 'friends' or strangers



Staff Observations Data

UID 101: Inexplicable Overseas Creditor

Customer is making frequent cross-border transfers of funds to the same creditor in overseas location with no apparent legitimate reason and inconsistent with customer's profile

Compliance Data
Transaction DataHigh-risk HT Source
CountriesHigh-risk CSE Facilitator
Countries

UID 330: Senior's Unusual Debit Activity



Withdrawals or purchases using ATM or debit cards that are inconsistent with an elderly customer's profile and prior usage patterns or times (e.g., late night or very early morning withdrawals by elder customers, withdrawals at ATMs in distant parts of town by customers who don't drive or are housebound)



Customer and Account Data
Compliance Data
Transaction Data

UID 330: Senior's Unusual Debit Activity



Withdrawals or purchases using ATM or debit cards that are inconsistent with an elderly customer's profile and prior usage patterns or times (e.g., late night or very early morning withdrawals by elder customers, withdrawals at ATMs in distant parts of town by customers who don't drive or are housebound)



Customer and Account Data
Compliance Data
Transaction Data

UID 339: Senior Confused about Financial Status Time



Senior appears to be confused about the financial status: account balance or transactions on the account. Customer has no knowledge of a newly-issued ATM, debit or credit card and is concerned about missing funds from their account



Staff Observations Data

UID 340: Cognitive Decline



Senior customer's physical or mental appearance changed, i.e., customer may appear uncharacteristically dishevelled, confused or forgetful. This could indicate self-neglect or early dementia and leave the individual vulnerable to financial exploitation



Staff Observations Data

UID 327: Senior with Sudden Non-sufficient Funds Activity



Senior with a stable account balance suddenly starts incurring non-sufficient funds (NSF) activity and related charges or showing low account balance



Compliance Data
Transaction Data

How to find it

Include steps 3 and 4 when assessing the risk of the elderly financial exploitation 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.

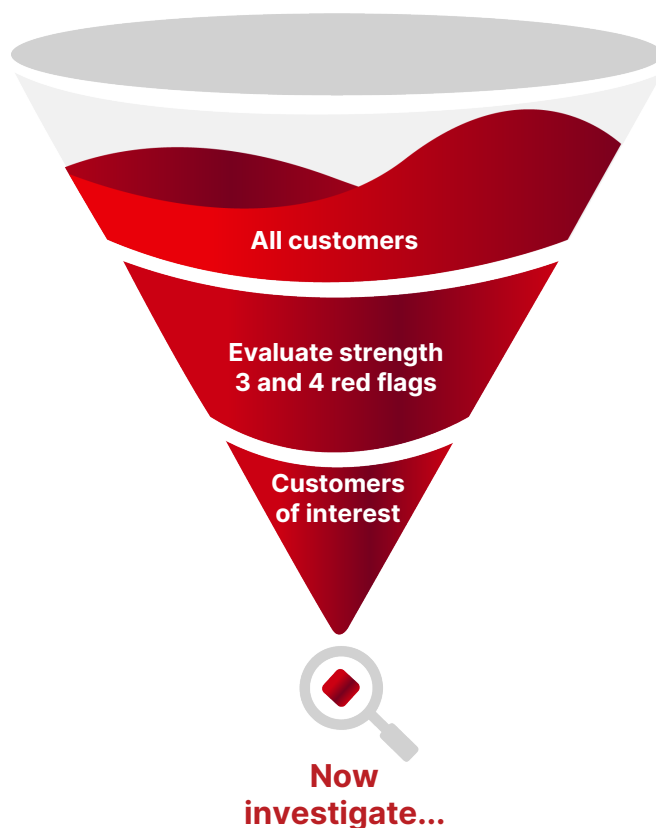
Gather the necessary external reference data to evaluate the red flags.

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 a trigger event has raised concern. This may be following step 4 or another trigger.

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 elderly financial exploitation by an unknown party 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

UID 328: ▶▶▶
Increased cash
withdrawals

RELEVANT STRENGTH 3 & 4 RED FLAGS

UID 336: ▶▶▶
Gift card activity

UID 337: ▶▶▶
Sudden change in
appointed fiduciaries

UID 334: ▶▶▶
Savings suddenly
withdrawn


RELEVANT STRENGTH 1 & 2 RED FLAGS


UID 101: ▶▶
Inexplicable overseas
creditor

UID 330: ▶▶
Unusual debit activity

UID 327: ▶
Sudden
Non-sufficient funds

NARROW DOWN POSSIBLE PERSONAS

 New cash
hoarder

 Elderly financial
exploitation
victim

 Legitimate
one-off cash
purchase

Investigation steps above illustrate an example where a TMS system has flagged an elderly customer for a sudden and significant recent increase in cash withdrawals.

- 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, three 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 elderly financial exploitation by unknown party – 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 elderly financial exploitation, 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 elderly financial exploitation. When raising a SAR, include all relevant supporting information for the identified red flags. In particular, FinCEN advise to:

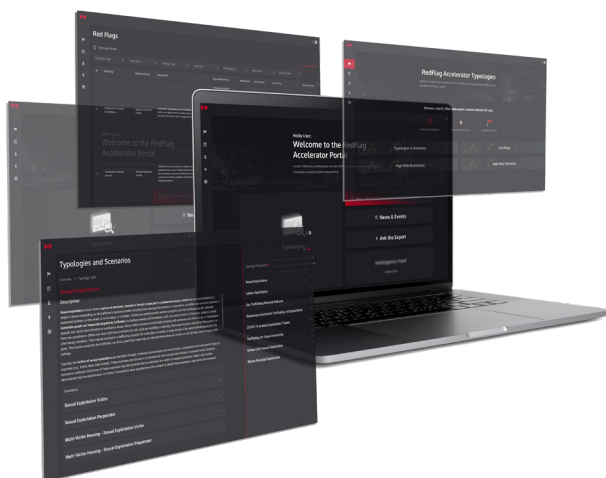
Take care in completing the narrative section of the report to provide a clear complete and concise description of the possible criminal activity.

Determine any obligations under state law to report the suspected activities to law enforcement and Adult Protective Services. When doing so, mark the law enforcement contact field within the SAR.

IN SAR Field 2, include 'EFE FIN-2022-A002' and reference the code in the narrative.

Mark the check box for Elder Financial Exploitation in SAR Field 38(d) as this will help law enforcement in their investigation.

Additionally, if the matter appears particularly time sensitive you may wish to call the Financial Institutions Toll-Free Hotline at (866) 556-3974 available 24 hours a day, 7 days a week.



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.

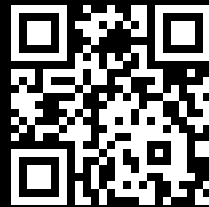
Contact us to learn about **Investigation and Detection Packs** including:

- 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