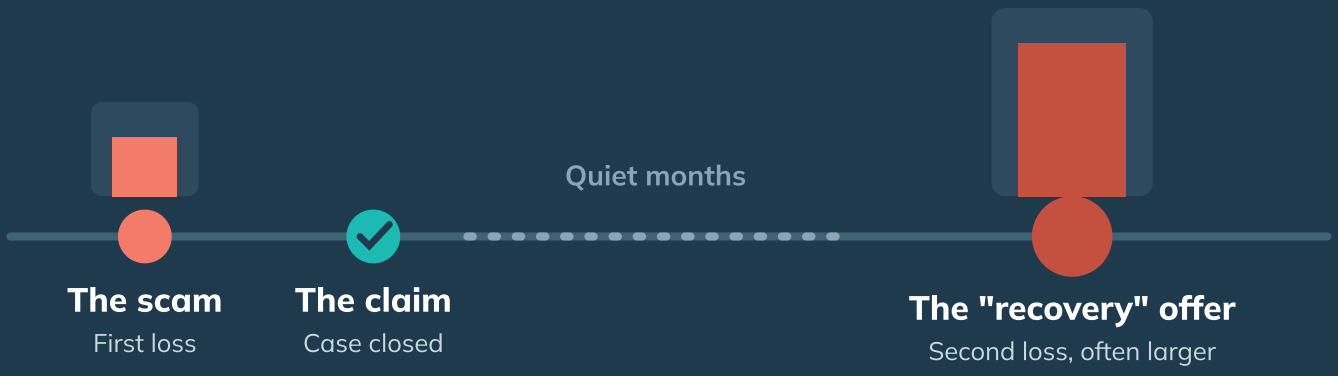
A PRACTITIONER'S GUIDE | EDITION 1, NOVEMBER 2026

From Scam to Recovery Scam

How to Spot and Stop the Second Hit in 5 Steps

A practitioner's guide for fraud and financial crime teams at banks, credit unions and building societies.



"We found your money. There is a fee to release it."

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
Flag	**Watch**	**Ask**	**Link**	**Warn**

Richard Stocks, Flggd

Flggd

Summary

When a customer loses money to a scam, the risk does not end with the claim. Criminals buy, sell and keep lists of people who have already paid, and they come back as lawyers, police, regulators or crypto tracers promising to recover the money for a fee. We call this the second hit.

It is measurable where anyone has looked. Action Fraud figures show £185.4 million lost to recovery scams in a year. Australian reports rose 129% on the six months before. The FBI has issued five warnings since 2023. Leaked call-centre records show the “lawyer” can be an employee of the operation that took the money in the first place.

Yet the second hit is usually logged as a new, unrelated case. No regulator tells institutions to treat a prior victim as higher risk, and the main US scam classification model has no category for it.

Five steps close the gap, and none needs new technology:

Flag	confirmed scam claimants as prior victims. 30 days.
Watch	for recovery-scam payment signals on flagged customers. 30 to 90 days.
Ask	open questions that get past coaching. Start Monday.
Link	the second hit to the first case, and report and share it. 30 days.
Warn	customers at claim time, and again. Start Monday.

The evidence says it works. Repeated warnings cut repeat victimisation by 22.4% in a randomised trial with the US Postal Inspection Service. The FBI’s free recovery route froze $679 million in 2025.

Two invitations close the paper: a page to give your customers, and a free benchmark to measure the second hit in your own book.

CONTENTS

1 The customer who comes back 4

2 What the second hit costs 6

3 Inside the recovery pitch 8

4 What fraud teams miss today 13

5 The 5 steps: Flag, Watch, Ask, Link, Warn 15

6 Proof that it works 20

7 For your customers 22

8 Measure it with us 23

About Flggd 24

Sources 25

CHAPTER 1

1 The customer who comes back

An illustrative case, built from the patterns in this paper. It is not a real customer.

Six months ago she reported an investment scam. She had sent £38,000 to a trading platform that turned out not to exist. Your team took the claim, did the work and closed the case.

This morning she adds a new payee, a law firm. They have found her money, they say, and they can get it back. There is a fee to release it.

Most fraud teams have seen this customer. Few have a name for what is happening to her. We call it **the second hit**: a recovery scam aimed at someone who has already lost money to a scam. It promises to undo the first loss, and it takes more.

FROM SCAM TO RECOVERY SCAM

The second hit: one customer, two losses



Source: illustrative; the bars show the shape of the pattern, not amounts

Figure 1

It is not rare, though no country counts it the same way. The figures below come from different bodies, periods and definitions. They should be read side by side, not added together.

- **United Kingdom.** 5,553 recovery scam reports and £185.4 million lost in the year to November 2025 (Action Fraud figures, reported by Which?, 13

November 2025).

- **Australia.** Scamwatch received 158 reports with a money recovery element from December 2023 to May 2024, 129% more than in the six months before. Losses were over A$2.9 million, a figure that includes what victims lost in the original scam (ACCC, 9 July 2024).
- **United States.** The FBI has issued five public warnings about recovery scams since 2023. In one year alone, crypto scam victims reported losing more than $9.9 million to fake law firms (FBI IC3, 24 June 2024).

THE SCALE

Three countries, three ways of counting the same crime



Different bodies, periods and definitions. Read side by side, never added together.

Source: Action Fraud via Which?, 13 Nov 2025; ACCC, 9 Jul 2024; FBI IC3 I-062424-PSA, 24 Jun 2024 Figure 2

Behind each number are people like the one Which? described in 2023. He lost £120,000 to an investment scam. Six months later he lost a further £560,000 to people who promised to get the first loss back (Which?, 11 September 2023).

It is tempting to treat the new payee as a new, unrelated case. It is not, and it costs more than the first.

CHAPTER 2

2 What the second hit costs

The customer pays first, and usually pays more. The second loss often lands on someone who has already borrowed, sold or emptied savings to fund the first. Because shame is heavier the second time, it is also the loss they are least likely to report.

The institution pays in three ways.

- **Trust.** The second hit arrives at the moment the customer most needs to believe their bank is on their side. A recovery scammer's best line is that the bank failed them and only the "law firm" can help.
- **Claims and complaints.** A second loss brings a second claim, a second complaint, or both, on a customer the institution already knows was targeted.
- **Exposure on the receiving side.** In Australia, the financial ombudsman can now examine the bank that received a scam payment as well as the bank that sent it (AFCA, from 12 March 2026). A recovery-scam payment has to land somewhere.

There is a third cost, and it belongs to the financial crime team. Victims who have lost money, and are told they can get it back, can be persuaded to move money for the people who took it. The US Justice Department puts it plainly: "Many money mules begin as victims of romance or lottery scams" (US Justice Department, 10 May 2024). The second hit can turn a fraud victim into an AML alert.

THE COST

Who pays for the second hit

The customer

- A second loss, often larger
- Often unreported: shame is heavier the second time

The institution

- Trust lost at the worst moment
- A second claim or complaint
- In Australia, the receiving bank can now be examined too

Financial crime

- Victims can be persuaded to move money for the scammers
- A fraud victim becomes an AML alert

Source: AFCA receiving-bank jurisdiction from 12 Mar 2026; US Justice Department, 10 May 2024 Figure 3

That makes the second hit a shared problem for fraud operations and financial crime teams. To stop it, you need to see how it works.

HOW WE KNOW

This paper draws on regulators in the US, UK and Australia; five FBI warnings issued between 2023 and 2026; leaked call-centre records published by OCCRP in 2020 and 2025; court and enforcement cases; a peer-reviewed study of scammers' own records; a randomised trial run with the US Postal Inspection Service; a UK payment-screen experiment; and real recovery-scam ads captured by Flggd.

Every figure is sourced at the back. Where advice rests on experience rather than a study, we say so.

3

CHAPTER 3

Inside the recovery pitch

Where the target comes from

A recovery scammer does not start cold. The FTC puts it plainly: “Refund and recovery scammers buy lists of people who’ve already been scammed, hoping they can be scammed again” (FTC, 3 August 2026). FINRA says the same: fraudsters “find their targets by purchasing or trading lists of people” (FINRA, 20 May 2024).

The trade in such lists is not a theory. In 2021 the US Justice Department reached a $150 million settlement with Epsilon, a data company whose employees “sold data associated to clients engaged in fraudulent mass-mailing schemes”; $127.5 million went to victims (US Justice Department, 27 January 2021). Similar cases followed against KBM Group and the list broker Macromark. Those lists fed mail fraud, not recovery scams. They show that a list of people likely to pay has a market price.

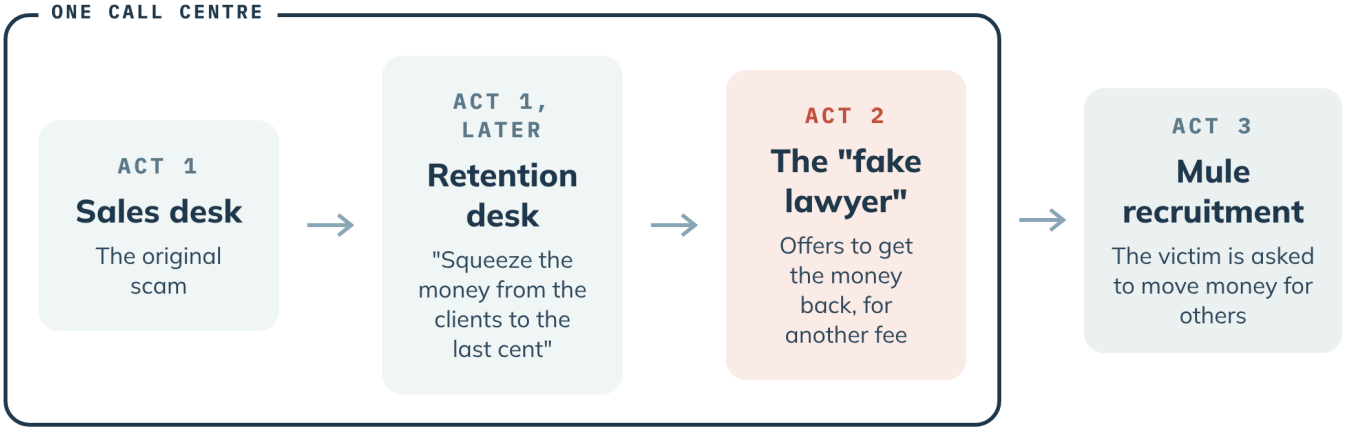
Often, though, the list never leaves the building. The CFTC describes fraud as three acts: the original scam, the recovery scam, then recruiting the victim to move money for others. “Many times, the same gang or a different one pulls off both the original and recovery scams” (CFTC, 30 July 2024).

Leaked call-centre records show how that works. In the Milton Group operation exposed by OCCRP, promising victims were passed to a “retention” desk whose staff aimed to “squeeze the money from the clients to the last cent”. Victims were then “contacted by fake lawyers offering to help get their money back, for yet another fee”. A whistleblower identified one victim’s “lawyer” as a Milton retention agent working under another name (OCCRP, 2 March 2020). The rescuer and the thief were the same company.

New Zealand’s regulator recorded the same pattern from the victim’s side. A man who lost more than NZ$20,000 to a share scam was approached by “recovery” firms whose offers “included accurate details of how many shares he bought and how much he had lost” (FMA, 1 May 2024). Only someone holding the original file could know that.

INSIDE THE PITCH

The rescuer and the thief can be the same company



A whistleblower identified one victim's "lawyer" as a retention agent from the same call centre. The CFTC: "the same gang or a different one pulls off both the original and recovery scams."

Source: OCCRP, Fraud Factory (Milton Group), 2 Mar 2020; CFTC release 8936-24, 30 Jul 2024 Figure 4

Four disguises

The pitch arrives in one of four forms:

- **A law firm** that specialises in fraud victims.
- **A government body or the police**, most often the FBI or its Internet Crime Complaint Center (IC3).
- **A regulator**, such as the FCA or ASIC.
- **A crypto tracing service** that promises to follow the money.

The FBI's own warnings track how far the disguises have come. In 2023 it warned about paid crypto "tracing" firms. In 2024 it warned about fake law firms claiming to work with the FBI and the CFPB. In 2025 it described scammers posing as fellow victims inside online support groups and steering people to a fake IC3 "Chief Director" on Telegram, calling the offer "a ruse to revictimize those who have already lost money to scams". In July 2026 it warned of AI deepfake video of a senior FBI leader directing victims to a spoofed IC3 website that issues its own reference numbers (FBI IC3 public service announcements, 2023 to 2026).

FOUR DISGUISES

Four disguises, and five FBI warnings that track how far they have come

A law firm
Specialises in fraud victims; free case review

Police or the FBI
Often the FBI or its IC3 complaint centre

A regulator
The FCA, ASIC or a made-up agency

A crypto tracer
Promises to follow the money



Source: FBI IC3 public service announcements, Aug 2023 to Jul 2026 Figure 5

IN THEIR OWN WORDS

Real recovery-scam ads aimed at people who have already lost money

SPONSORED
"If you're a victim of online fraud, reach out. Our law firm is one of the most..."
Red flag: Sponsored. Targets victims by name of the harm

SPONSORED
"Cryptoscam? Romancescam? Pigbutchering? Confidential case evaluation at no cost."
Red flag: Free 'evaluation' opens the conversation

SPONSORED
"Been scammed? Let us help you fight back and recover what's rightfully yours."
Red flag: Asks if you have been scammed

SPONSORED
"Fees are charged only for successful recovery."
Red flag: The fee comes later, as 'release' or 'tax'

SPONSORED
"We have successfully handled 1000++ scam case with recovery... only accept victim who haven't hire a lawyer."
Red flag: Unverifiable success claim; wants victims with no lawyer

SPONSORED
"Direct access to elite fraud recovery lawyers. We fight to recover stolen assets..."
Red flag: No firm registration or bar details

Ad text as captured, spelling as published. Firm names removed. Screenshots, with names and faces blurred, replace these cards in the final edition.

Source: real sponsored social media ads captured by Flggd, October 2026 Figure 6

The sales floor

Recovery is not an improvised side line. It is run like a sales team.

Milton Group agents made up to 300 calls a day against monthly desk targets of $40,000 for Russian speakers, $60,000 for Spanish and $100,000 for English. They earned more commission when victims paid in bitcoin. Agents were “carefully taught to sell ‘emotions’”, and the guidance for some clients was that “the only way to handle such people is not to argue with them” (OCCRP, 2 March 2020).

The 2025 Scam Empire leak, from call centres in Georgia and elsewhere, shows the same discipline five years on. Teams worked to targets such as “process 30K per day” and “$420,000 for the month”, with leaderboards and bonuses tied to money taken. One English-language retention desk “earned over $15.6 million” in a year. And when a victim saw through it, the instruction from a supervisor was not to let go: “This client realized it’s a scam. Don’t go today without calling them. Call and get the money” (OCCRP, 5 March 2025).

THE SALES FLOOR

Run like a sales team: targets, leaderboards and bonuses

300
calls a day per agent (Milton Group, 2020)

$100k
monthly target for the English-language desk (Milton Group)

$420k
monthly target for one team (Scam Empire, 2025)

$15.6m
earned in a year by one retention desk (Scam Empire)

"This client realized it's a scam. Don't go today without calling them. Call and get the money."
A supervisor's instruction, from the leaked records

Source: OCCRP, Fraud Factory, 2 Mar 2020; OCCRP, Scam Empire, 5 Mar 2025 Figure 7

Why customers pay again

None of this would work if victims did not respond. They do, for reasons that have little to do with intelligence.

Gambling research has a name for the pull: chasing, defined as going back “to get even” after a loss (DSM-5, quoted in Auer and Griffiths, 2023). A recovery offer is an invitation to get even on one specific loss. The link to fraud is our analogy, not a tested finding, but research on chronic fraud victims describes the same pull: “a

recurring hope that the next ‘opportunity’ that presents itself will succeed”, alongside “doubling down on secrecy” (AARP and FINRA Foundation, 3 March 2021). Shame keeps the second loss quieter than the first.

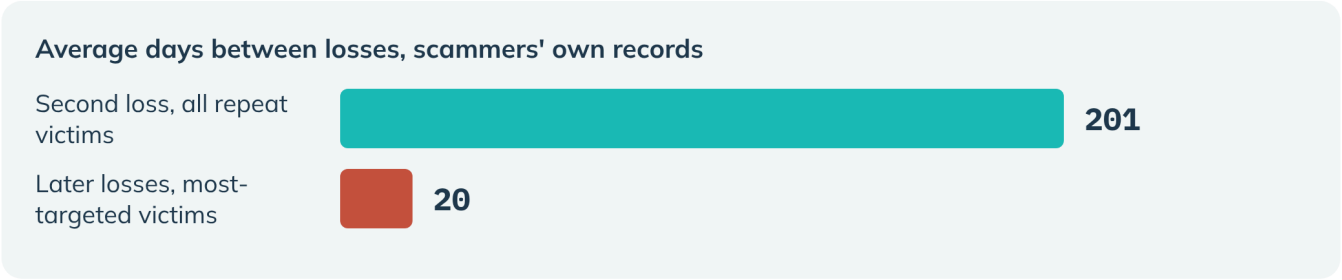
How often the pitch lands is rarely measured. The nearest public figure comes from the FCA. Of 10,379 people who reported contact from fake FCA staff in 2024, 991 paid. That is about 1 in 10 (our calculation from FCA figures, 27 August 2025), and it covers every kind of FCA impersonation, not only recovery offers.

The scammers’ own records show what happens over time. In four databases seized from mail-fraud operations, covering more than 1.3 million victims, 62% were defrauded more than once. Fewer than 1 in 10 victims, the most heavily targeted, produced 62% of the scammers’ revenue, and for them the gap between losses shrank from about 201 days to about 20 (NIJ and RTI International, 13 January 2025). That is mail fraud, not recovery fraud. It shows the principle: a first loss marks a person, and the next approach comes faster.

The scammers are organised, targeted and patient. On the institution’s side, the second hit usually arrives as a new case with no link to the first. That gap is where it gets through.

WHY CUSTOMERS PAY AGAIN

A first loss marks a person, and the next approach comes faster



62%
of victims were defrauded more than once

1 in 10
who reported fake FCA contact paid (our calculation)

The NIJ/RTI data covers mail fraud from 1999 to 2018, not recovery scams; it shows the pattern of repeat targeting.

Source: NIJ / RTI International, 13 Jan 2025; FCA, 27 Aug 2025 (991 of 10,379 in 2024) Figure 8

4

CHAPTER 4

What fraud teams miss today

None of the gaps below is a failure of effort. Each is a gap in how the work is set up.

The second hit is logged as a new case. A customer's scam claim is closed. Months later a new payee or a new payment trips an alert, and an analyst opens a fresh case with no link to the first. The context that matters most, that this customer has already been targeted, is not in front of the person deciding.

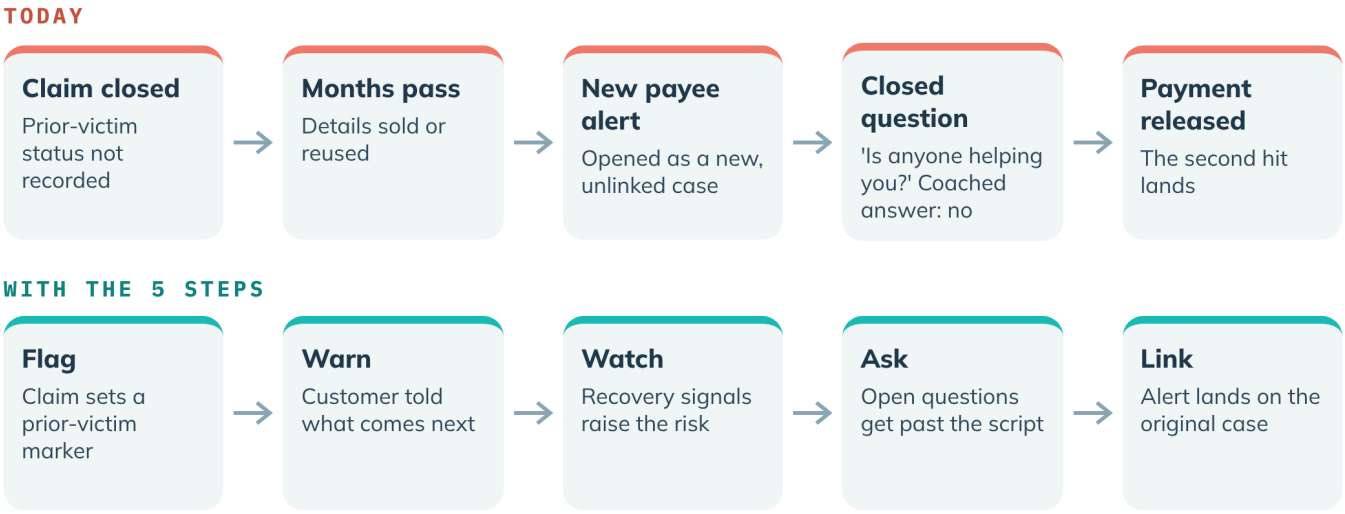
It cannot be counted. The Federal Reserve's scam classification model, which many US institutions use to categorise scams, has nine scam types and no category for recovery scams. A recovery scam is logged as an impostor scam or something else. What is not counted is not managed.

Nobody has told institutions to treat prior victims differently. We found no regulator in the US, UK or Australia that tells institutions to treat a customer with a confirmed scam claim as higher risk. The 2024 US Interagency Statement on Elder Financial Exploitation does not mention recovery scams. The UK ombudsman decisions we reviewed on recovery-scam payments did not consider whether the bank knew the customer had already been scammed.

The check the customer is given has been rehearsed. Interventions often rest on closed questions: is anyone helping you, did anyone tell you to do this. Scammers coach victims to answer them. One leaked instruction reads: "Tell them, no, I did it by myself, okay?" (OCCRP, 5 March 2025). A customer who has been coached passes a yes-or-no check every time.

WHAT FRAUD TEAMS MISS TODAY

Where the link is lost, and how the 5 steps keep it



Source: chapter 4; the coaching line is from OCCRP, Scam Empire, 5 Mar 2025

Figure 9

> **“Tell them, no, I did it by myself, okay?”**

Each of these gaps has a fix, and none needs new technology. There are five.

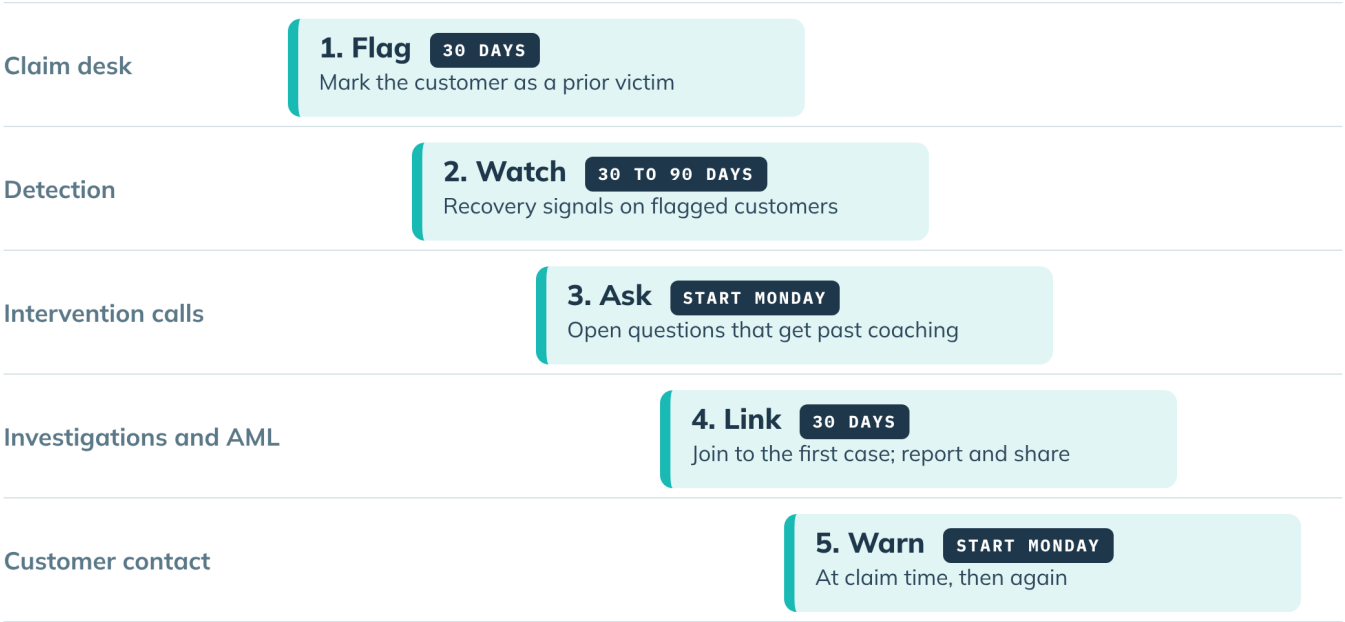
CHAPTER 5

5 The 5 steps: Flag, Watch, Ask, Link, Warn

Each step closes one of the gaps in chapter 4. Each says what to do, why, what it needs and how long it takes to start. Where a step rests on a published source, we cite it. Where it rests on experience, we say “practitioner judgement”.

THE 5 STEPS

Flag, Watch, Ask, Link, Warn: who does what



Source: chapter 5; effort tags are practitioner judgement

Figure 10

Step 1. Flag

What. When a scam claim is confirmed, mark the customer as a prior victim. Make the marker visible to everyone who decides on that customer’s payments and alerts: fraud operations, detection, and the AML team.

Why. A first loss is the strongest known predictor of the next one. In scammers’ own records, 62% of victims were hit more than once (chapter 3). Recovery scammers work from lists of people who have already paid.

How long. Keep the flag for 12 to 24 months and review it at the end, extending it if the customer is targeted again (practitioner judgement; no published source sets a window).

What it needs. Data you already hold: confirmed claims. A field or tag in the customer record and case system.

EFFORT 30 DAYS

Step 2. Watch

What. For flagged customers, raise the risk on the payment signals that mark a recovery scam:

- a new payee described as a law firm, solicitor, attorney, “recovery”, “asset tracing” or “fraud recovery” service;
- payment references or descriptions such as fee, tax, release, clearance, unlock, retainer or legal costs. FinCEN lists payments described as “taxes”, “fees” or “penalties” as a red flag (FinCEN, FIN-2023-Alert005);
- first-time crypto activity, or payments to a crypto exchange, after a claim (FinCEN, FIN-2023-Alert005);
- several payments to the same new payee in a short window. In gambling research, several deposits in one session is the strongest sign of chasing losses; we apply it here as practitioner judgement;
- a “recovery” firm that should be authorised and is not. In the UK, “A firm must be authorised by us to advertise or undertake these services” (FCA, updated 19 January 2026). In the US, telemarketers may not charge a fee to recover money already lost until seven business days after it is returned (Telemarketing Sales Rule, 16 CFR 310.4(a)(3)); licensed attorneys are exempt, which is one reason the fakes pose as law firms.

What it needs. Rule changes in your existing monitoring, scoped to flagged customers so the alert volume stays small.

EFFORT 30 TO 90 DAYS

STEP 2: WATCH

Five signals to watch on a flagged customer's payments

1	New payee: law firm, solicitor, attorney, 'recovery' or 'asset tracing'	PRACTITIONER JUDGEMENT
2	References: fee, tax, release, clearance, unlock, retainer	FINCEN FIN-2023-ALERT005
3	First-time crypto, or payments to an exchange, after a claim	FINCEN FIN-2023-ALERT005
4	Several payments to the same new payee in a short window	PRACTITIONER JUDGEMENT, FROM GAMBLING RESEARCH
5	A 'recovery' firm that should be authorised and is not	FCA; US TELEMARKETING SALES RULE

Scope the rules to flagged customers so the alert volume stays small.

Source: FinCEN FIN-2023-Alert005; FCA recovery room page, 19 Jan 2026; 16 CFR 310.4(a)(3); Auer and Griffiths, 2023 Figure 11

Step 3. Ask

What. When a flagged customer's payment is stopped, ask open questions that a coached customer cannot answer from a script:

- "How did this firm first contact you?"
- "Who told you how much you will get back?"
- "Did they give you a case or reference number? Where did it come from?"
- "Have you been asked to install anything or share your screen?"
- "Who else have you told about this?"

Listen for the phrases the FBI and others have documented: the money "has been found" or "recovered"; the FBI, IC3, a regulator or a law firm "is handling my case"; there is a fee or tax to "release" the funds (FBI IC3, 2024 and 2025).

Why. Closed questions are rehearsed (chapter 4). Open questions make the customer tell the story, and the story is where a recovery scam shows (practitioner judgement).

What it needs. A one-page script and a short briefing for the teams who make intervention calls.

EFFORT START MONDAY

STEP 3: ASK

Questions a script can answer, and questions it cannot

Closed: easy to coach

Is anyone helping you with this payment?

Did anyone tell you to make it?

Are you sure you want to go ahead?

Do you know the person you are paying?

Scammers rehearse these: "Tell them, no, I did it by myself, okay?"

Open: the story shows the scam

How did this firm first contact you?

Who told you how much you will get back?

Did they give you a case or reference number? Where did it come from?

Have you been asked to install anything or share your screen?

Who else have you told about this?

Listen for: "the money has been found", "the FBI is handling my case", "there is a fee to release it".

Source: OCCRP, Scam Empire, 5 Mar 2025; FBI IC3 warnings 2024 and 2025; questions are practitioner judgement Figure 12

Step 4. Link

What. Treat the second hit as part of the first case. Join them on shared phone numbers, email addresses, domains, crypto wallets and receiving accounts, and on timing. Then:

- in the US, use the suspicious activity report key terms that exist today, “EFE FIN-2022-A002” for elder exploitation and “FIN-2023-PIGBUTCHERING” where it applies, and the elder checkbox (FinCEN; Interagency Statement, 4 December 2024);
- share indicators with other institutions under section 314(b) in the US, or through the Australian Financial Crimes Exchange and Fraud Reporting Exchange in Australia (Scam-Safe Accord);
- check whether the customer is now being asked to receive or move money for others (chapter 2).

Why. The same people often run both scams (chapter 3), and the infrastructure links them. A linked case gives the investigator the whole picture and gives other institutions something to act on.

What it needs. A case-linking rule in your case management system and a habit in the investigation team.

EFFORT 30 DAYS

Step 5. Warn

What. When a scam claim is made, tell the customer what will happen next. Use the words the FBI uses: “Law enforcement does not charge victims a fee for investigating crimes” (FBI IC3, 24 June 2024). Tell them their details may now be

on a list sold to other criminals. Tell them the institution will only contact them through channels they already know. Give them the free routes: their bank, the police reporting service, the ombudsman. Tell them: “No genuine agency, police force or bank charges you a fee to get your money back.”

Then warn them again, more than once, over the following months.

Why. Chapter 6 shows that repeated reminders to past victims cut repeat victimisation.

What it needs. A claim-time script, a follow-up message schedule, and the customer page in chapter 7. The public guide for customers is at www.flggd.com/recovery-scams.

EFFORT START MONDAY

STEP	WHAT	EFFORT
Flag	Mark confirmed scam claimants as prior victims, visible to fraud and AML	30 days
Watch	Recovery-scam payment signals for flagged customers	30 to 90 days
Ask	Open questions that get past coaching	Start Monday
Link	Join the second hit to the first case; report and share	30 days
Warn	Tell them at claim time, then again	Start Monday

Each step is cheap. The next question is whether any of it works.

6 CHAPTER 6
Proof that it works

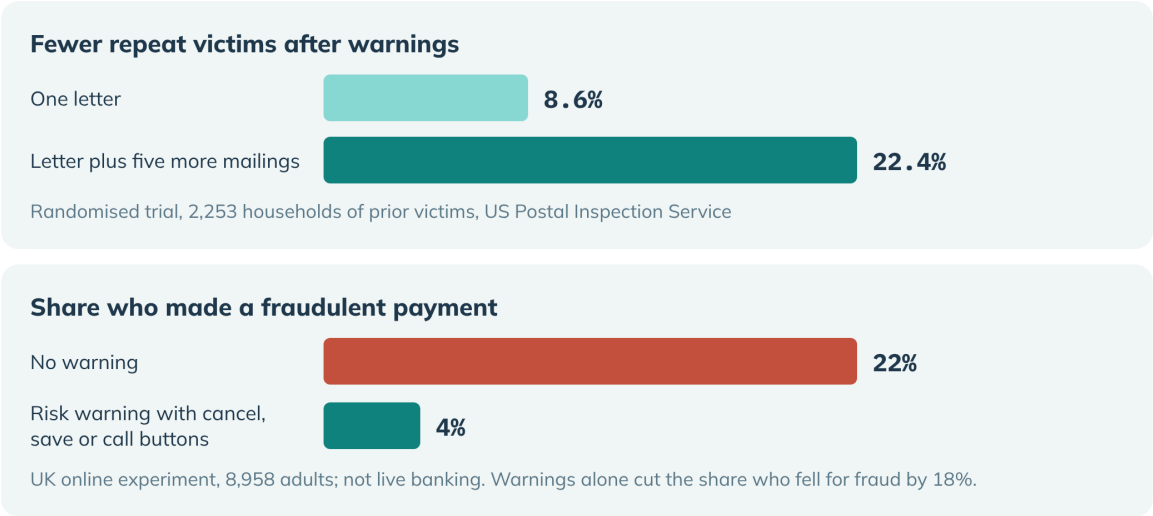
It does.

Repeated warnings cut repeat losses. The US Postal Inspection Service ran a randomised trial with 2,253 households that had already lost money to mail scams. One warning letter cut repeat victimisation by 8.6%. The letter plus five more awareness mailings, sent two weeks apart, cut it by 22.4% over four months. The result was measured from scam mail that inspectors intercepted, not from what people said about themselves (DeLiema, Langton and others, Journal of Consumer Affairs, 2026). That is the evidence behind Warn, and behind saying it more than once.

Friction works better than words alone. In a UK experiment run with the Open Banking Implementation Entity, with 8,958 adults, behavioural warnings cut the share who fell for fraud by 18%. A risk-based warning with buttons to cancel, save for later or call the bank cut fraudulent payments from 22% in the control group to 4% (Akesson, Gathergood and Quispe-Torreblanca, University of Nottingham CeDEx Discussion Paper 2023-08). It was an online experiment, not live banking, but it points the same way as Watch and Ask: give the customer a reason and a way to stop.

PROOF THAT IT WORKS

Repeated warnings and real friction both cut losses



Source: DeLiema, Langton and others, Journal of Consumer Affairs, 2026; Akesson, Gathergood and Quispe-Torreblanca, CeDEx DP 2023-08

Figure 13

The real recovery route is free, and it works. The FBI's Recovery Asset Team works with banks to freeze money after a reported fraud. In 2025 it froze $679 million of $1.16 billion it tried to stop (FBI IC3, Internet Crime Report 2025). That is the route a customer should be pointed to, and it costs them nothing.

THE REAL RECOVERY ROUTE

The real recovery route is free, and it works



Source: FBI IC3, Internet Crime Report 2025; IC3 I-062424-PSA, 24 Jun 2024 Figure 14

Disruption moves a whole scam type. In Australia, reports of remote access scams fell 47.8% in 2025, which the National Anti-Scam Centre attributes to "detection and disruption efforts of banks and the telecommunications sector" (NASC, Targeting Scams 2025). Banks have moved a scam category before.

Much of the work is a conversation with the customer. Here is the page to give them.

CHAPTER 7

7 For your customers

This page is yours to copy and give to any customer who has been scammed.

FOR CUSTOMERS WHO HAVE BEEN SCAMMED

You may be contacted again

Scams happen to careful people. You did the right thing by telling us.

Now be ready for a second approach. People who have lost money to a scam are often contacted by someone who says they can get it back. They may say they are a lawyer, the police, the FBI, a regulator or a firm that traces money. They may know how much you lost. They are not there to help.

THREE RULES

1 Never pay to get your money back.

No genuine agency, police force or bank charges you a fee to get your money back. "Never pay up front for a refund...or for help getting one" (FTC). "No genuine agency charges upfront fees to return stolen funds" (IDCARE).

2 Check the firm yourself.

Look it up on the official register, not through a link or number they give you.

3 Only use routes you find yourself.

Your bank, the police reporting service and the ombudsman are free.

Your details may now be on a list sold to other criminals. We will only contact you through channels you already know.

WHERE TO GET HELP

UNITED STATES

Report: ic3.gov

National Elder Fraud Hotline: 833-FRAUD-11 (833-372-8311)

AARP Fraud Watch Network Helpline: 877-908-3360

UNITED KINGDOM

Call 159 to reach your own bank safely

Report: reportfraud.police.uk or 0300 123 2040 (England, Wales and Northern Ireland)

Victim Support: 08 08 16 89 111

AUSTRALIA

Report: scamwatch.gov.au, or ReportCyber at cyber.gov.au

IDCARE: 1800 595 160

Money just moved? flggd.com/emergency. More help: flggd.com/recovery-scams.

8

CHAPTER 8

Measure it with us

Nobody publishes how often the second hit lands. The only national figure we found is old: in England and Wales, 86% of fraud victims were victims once, which leaves about 14% hit more than once (ONS, March 2017, cited by the Home Office in 2018; the 14% is our calculation). The Home Office itself warns that this "may hide true levels of repeat victimisation".

Every institution already holds the data to do better. We propose four measures:

MEASURE	HOW TO CALCULATE IT
Re-victimisation rate	Confirmed scam claimants with a second confirmed scam loss within 12 months, divided by all confirmed scam claimants
Time to re-contact	Median days from the first confirmed loss to the first recovery approach seen or reported
Intercept rate	Recovery-scam payments stopped for flagged customers, divided by all recovery-scam payments attempted by flagged customers
Mule conversion	Prior victims later seen receiving or moving money for others, divided by all prior victims

Run them in your own book, and you will know the size of your second-hit problem within a quarter.

We would like to go further. Flggd will run an anonymised benchmark: institutions share these four measures, and we publish the results so everyone can see how they compare. It is free to join.

About Flggd

Flggd is designed for credit unions, community banks, building societies and member-owned institutions, where protecting customers matters to everyone. People check suspicious messages with Flggd, and scammers' own messages, links and ads feed the Flggd Brain. The Brain feeds what it learns back to people and to the institutions that serve them.

ABOUT FLGGD

What feeds the Flggd Brain, and what it feeds back



Three things to do next

Join the benchmark.

Share the customer page, or the guide at www.flggd.com/recovery-scams.

flggd.com/book-a-call

Richard Stocks gathers and shares what the industry knows about scams. He has spent 25 years in financial crime, AML and fraud technology.

Sources

Wording and figures were checked on the dates shown. Items marked * were read through secondary reporting or a summarising tool and are confirmed against the original before publication.

REGULATORS AND GOVERNMENT

ACCC / National Anti-Scam Centre. “Criminals targeting victims of previous scams promising financial recovery.” 9 July 2024. accc.gov.au*

National Anti-Scam Centre. Targeting Scams Report 2025. March 2026. nasc.gov.au*

AFCA receiving-bank jurisdiction from 12 March 2026, as reported by MinterEllison and IDCARE.*

CFTC. Release 8936-24, “CFTC Warns Customers to Watch for Follow-on Frauds.” 30 July 2024. cftc.gov*

FBI IC3. Public service announcements I-081123-PSA (11 Aug 2023), I-062424-PSA (24 Jun 2024), I-041825-PSA (18 Apr 2025), I-081325-PSA (13 Aug 2025), I-072026-PSA (20 Jul 2026). ic3.gov*

FBI IC3. Internet Crime Report 2025 (Recovery Asset Team). ic3.gov*

FCA. “Fake FCA scams reported in first 6 months of 2025.” 27 August 2025. fca.org.uk*

FCA. Recovery room fraud page, updated 19 January 2026. fca.org.uk*

Federal Reserve. ScamClassifier model. fedpaymentsimprovement.org*

FinCEN. Advisory FIN-2022-A002, elder financial exploitation. 15 June 2022.*

FinCEN. Alert FIN-2023-Alert005, pig butchering. 2023.*

FMA (New Zealand). “No rest for the scammed: recovery room fraudsters prey on victims.” 1 May 2024. fma.govt.nz*

FTC. “Have you lost money to a scam? Watch for scammers who say they can help.” 3 August 2026. consumer.ftc.gov*

FTC. Telemarketing Sales Rule, 16 CFR 310.4(a)(3). ecfr.gov*

Federal Reserve, CFPB, FDIC, FinCEN, NCUA, OCC and state regulators. Interagency Statement on Elder Financial Exploitation. 4 December 2024.*

Home Office. “The scale and nature of fraud: a review of the evidence” (2018), citing ONS (March 2017). gov.uk*

US Justice Department. Epsilon deferred prosecution agreement, 27 January 2021; KBM Group, 15 June 2021; Macromark, 28 September 2020. justice.gov*

US Justice Department. Money mule initiative statement, 10 May 2024. justice.gov*

UK Financial Ombudsman Service. Decisions DRN-4853300 and DRN-4844652.*

Australian Banking Association and COBA. Scam-Safe Accord. 2023. ausbanking.org.au*

RESEARCH

AARP and FINRA Investor Education Foundation. Chronic fraud victimisation study. 3 March 2021.*

Auer, M. and Griffiths, M. D. (2023), on chasing losses in gambling, quoting DSM-5.*

Cross, C., Richards, K. and Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. Australian Institute of Criminology.*

DeLiema, M., Langton, L. and others (2026). “Be a Fraud Fighter” randomised trial with the US Postal Inspection Service. Journal of Consumer Affairs, DOI 10.1111/joca.70059; sample of 2,253 addresses from the NIJ grant report, ojp.gov/pdffiles1/nij/grants/308661.pdf*

NIJ / RTI International. “Insights on mail fraud from scammers’ own records.” 13 January 2025. nij.ojp.gov*

Akesson, J., Gathergood, J. and Quispe-Torreblanca, E. (2023). CeDEx Discussion Paper 2023-08, University of Nottingham, in collaboration with the Open Banking Implementation Entity. nottingham.ac.uk*

INVESTIGATIONS AND OTHER SOURCES

FINRA. “Recovery scams.” 20 May 2024. finra.org*

OCCRP. “Fraud Factory” (Milton Group). 2 March 2020. occrp.org*

OCCRP. “Scam Empire.” 5 March 2025. occrp.org*

Which?. “Don’t get scammed twice.” 11 September 2023. which.co.uk*

Which?. Recovery scammers on Trustpilot, citing Action Fraud figures. 13 November 2025. which.co.uk*

Flggd. Recovery-scam advertisements captured October 2026; firm names removed.