LOVESAID

2025

WHAT BANKS NEED TO KNOW
ROMANCE FRAUD

A Guide for Financial Institutions:
Detection, Empathy & Disruption

Prevent. Support. Empower.

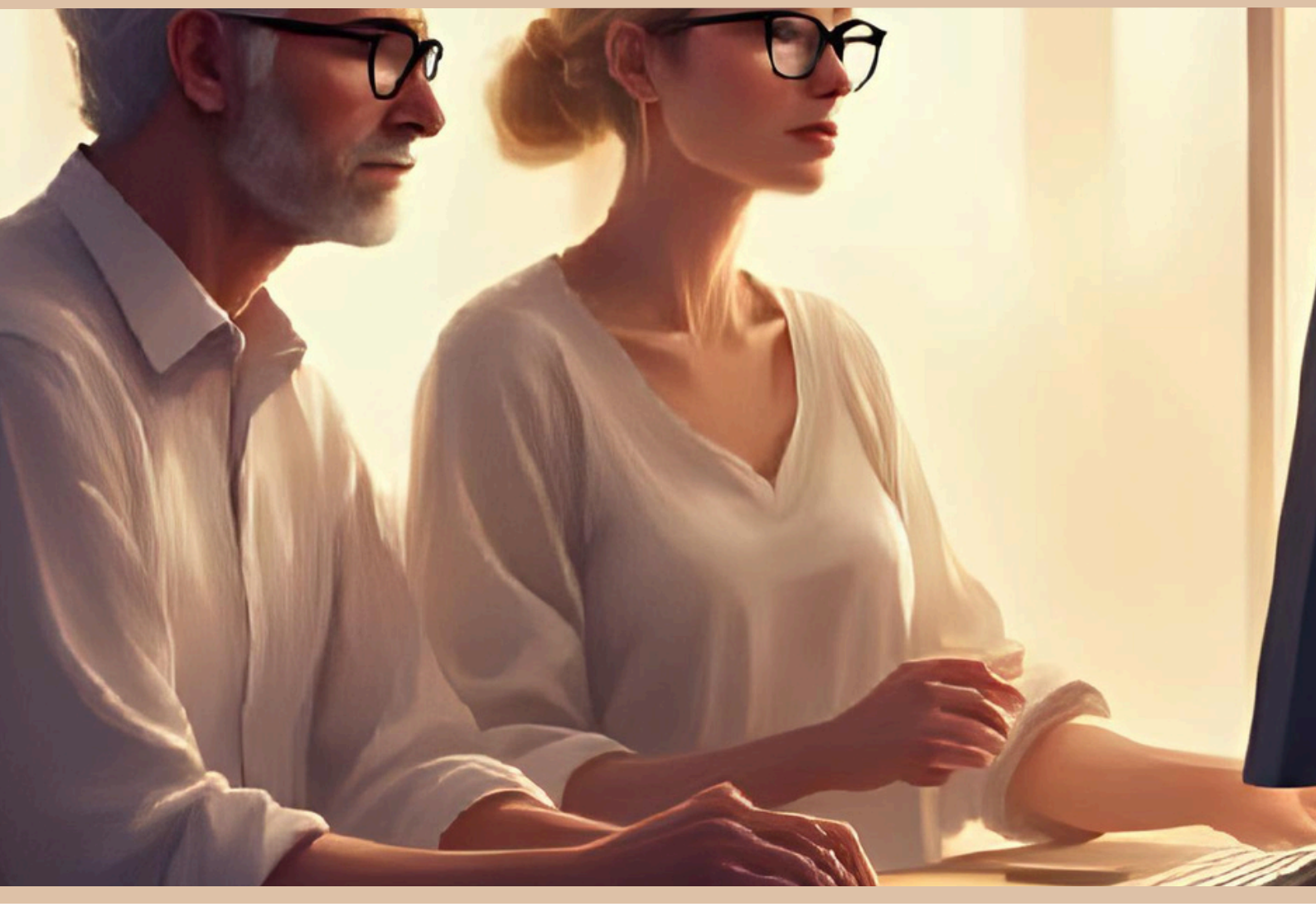


TABLE OF CONTENTS

1 Messages from victims

2 What is Romance fraud?

3 Where does it start?

4 Emotional Manipulation

5 Recognising Coercion and coached Q & A's

7 Transactions 'red flags' and patterns.

8 Engaging with emapthy and Safeguarding victims

10 Let's Work Together

MESSAGES FROM VICTIMS

As someone who's been through the trauma of a romance scam, I can honestly say Nationwide were outstanding in how they handled my situation. They treated me with kindness and respect, and most importantly, they didn't close my account, which would have added an enormous amount of stress at an already overwhelming time.
They went above and beyond to make sure I was safeguarded against future scams, even putting special checks in place for my transactions. Yes, it can be a bit of a pain at times, but I completely understand why, it's there to protect me.
I felt genuinely supported, not judged, and that made all the difference in starting to rebuild. Thank you, Nationwide, for helping me feel safe again.

CC

Victim of Online Romance Fraud

My experience with my bank following the scam was almost as distressing as the scam itself. I was made to talk about what happened in the middle of the customer hall, with no privacy or sensitivity whatsoever. When I explained the situation, the staff member looked at me and said, "Well, you willingly sent the money, I don't know what you expect us to do about it."
There was no clear process to help me file a reimbursement claim, and I was left chasing updates well beyond the time limits for a final response. To make things worse, they closed my account completely, claiming it had been used as a "mule account." I had no idea that's what those transactions were, and yet I was treated like a criminal instead of a victim.
The whole experience was humiliating, isolating, and utterly lacking in care or understanding. No one should be made to feel that way when they're already vulnerable and traumatised.

MS

WHAT IS
ROMANCE FRAUD?

It is not a victim who gives their money away willingly. There is always emotional manipulation and coercion to make the victim seemingly complicit and compliant.

While ‘sextortion’ can be part of romance fraud, its introduction into the scenario created by the criminal and the speed at which this occurs is very different to the stand alone ‘sextortion’ cases we see. The blackmail element of this will rarely occur until the end of the fraud, many months down the line when the criminal is having one last attempt to intimidate the victim into sending more money. Typical stand alone sextortion cases will occur over a 24-48 hour period.

Romance fraud is a deeply manipulative crime where perpetrators use powerful emotional tactics to create a fake reality around their victims. Through intense love, trust, and devotion, fraudsters construct an immersive theatre of deception, making victims emotionally invested in a relationship that doesn’t truly exist. This manipulation makes victims compliant and even seemingly complicit in the fraud, despite being the ones deceived and exploited.

The impact of romance fraud extends far beyond financial loss. The emotional trauma is profound, victims not only have money stolen, but also experience a deep betrayal of trust, both in others and in themselves. The loss of what feels like the most intense relationship of their lives can be devastating, leading to long-term psychological effects such as shame, grief, and identity crisis.

Recovery from romance fraud is a long journey. Ensuring that victims experience as little additional stress as possible is crucial to their healing. Providing compassionate support, reducing blame, and offering clear guidance can help victims rebuild their lives and regain their sense of trust and self-worth.

WHERE **DOES IT START?**

What does Romance Fraud look like?

There are three, some may classify four distinct MO's of romance fraud. First is online romance fraud, from overseas locations (may have UK elements or perpetrators). Second, Romance/Investment Hybrid (aka- 'Pig Butchering'). Third, In- person romance fraud. Lastly, marriage fraud.
Every victim, whatever the MO, will have gone through a journey of manipulation. It starts here:

When in a state of situational vulnerability such as grieving, being lonely, anxious or changes in life situations, our brains become flooded with a potent chemical cocktail: dopamine, oxytocin, cortisol, and adrenaline. These hot states heighten emotional responses and impair critical thinking. It opens the door for manipulation because we are seeking relief and love.

When falling in love, the brain's reward system lights up, making us bond deeply, quickly, and often being less risk averse. Add to that a range of cognitive biases, like optimism bias, confirmation bias, and the sunk cost fallacy, and we begin to blur harmful behaviours, red flags are seen as beige, to protect the hope we've invested. In these moments, we don't question the abuser or fraudster, we question ourselves. And that's exactly how manipulation takes hold.

EMOTIONAL MANIPUALTION

- Grooming: Much like the grooming of minors, the criminal will open up to the victim and talk about their own past and anxieties. This gives a sense of trust to the victim to open up about themselves and their own history-of course the criminal's version is a fabricated story. During this time, the criminal will draw out and record things that can be used to further the fraud at a later date and also begin the attachment/hooking process by mirroring the victim with good and sad experiences, beliefs, morals and ethics.

- Love Bombing: The victim is bombarded with attention and affection and even gifts. The criminal will make the victim feel that they are at the centre of their world and the most important person in it. Victims who suffer with low self esteem or self worth are particularly susceptible to this manipulation as it gives them confidence in themselves, when they have none.

- Trauma Bonding 1: The criminal may ask something of the victim to test them. If the victim does not respond in the way the criminal requires, they will withdraw contact for a period of time. The trauma this causes after the intense communication and affection that has preceded this, has the effect of bonding the victim further by ensuring that further requests are responded to in a more favourable way (this does not have to be financial).

- Trauma Bonding 2: This technique as the name suggests, bonds the victims through a similar experience. The feeling of shared understanding is a powerful manipulation.

- Trauma bonding 3: This is part of the fraud where the bigger ask is requested but attached to something traumatic. It might be ill health, a brush with the law, the loss of access to funds to complete a contract that has been worked on for months etc.

Within these manipulations will be elements of coercive and controlling behaviours including isolation and slow and subtle building of an alternate reality. These manipulations parallel those behaviours used in domestic abuse relationships.

Romance Fraud

Romance fraud is not a fringe issue. It is a growing, organised, and psychologically complex crime that moves billions globally, and banks sit at the intersection between the abuse and the financial harm.

Banks are not just bystanders. With the right awareness and tools, they can become a critical line of defence.

Recognising Psychological Coercion

Many victims are coached by the scammer on what to say when questioned:

- "It's for a friend in need."
- "I'm helping someone with travel costs."
- "I met them online, we're engaged."
- "It's a private matter."

These answers are not signs of awareness. They are often signs of grooming and coercion. Victims may appear agitated, defensive, or overly trusting. But underneath is a trauma bond, and fear of losing someone they believe they love.

Romance Fraud Coaching Questions

Recognise Coercion and Disrupt Fraud

Victims of romance fraud are often *coached* by criminals to respond to bank staff in ways that sound plausible, polite, or confident. These rehearsed statements are not evidence of informed consent, they are a symptom of coercion, trauma bonding, and manipulation.

This guide helps bank staff recognise common scripts, understand the underlying manipulation, and respond with phrases that break the illusion and support victim safety.

Common Coached Statements and How to Respond

1. **"It's just a personal loan to a friend."**

What's really happening: The "friend" is likely a criminal. The victim has been manipulated into believing it's a short-term loan.

Disruptive response:

- "Have you ever met this friend in person? Sometimes people online build trust with the goal of financial exploitation. We see cases like this every day. Can we help you pause and verify some details before continuing?"

2. **"It's for someone I'm in a relationship with- we're engaged."**

What's really happening: Emotional grooming and love bombing are at play. The victim is in a trauma bond.

Disruptive response:

- "We understand relationships can move fast, especially online. Would you be open to a few checks that might confirm this person's identity? Many scammers build fake relationships for months before asking for money."

Coached Statements continued

3. **"They're stuck abroad and need help. I'm the only one they can turn to."**

What's really happening: This is a classic fraud scenario, often with fake travel, hospital, or visa stories.

Disruptive response:

- "This exact situation, someone abroad urgently needing money-matches a common fraud pattern. It doesn't mean you've done anything wrong, but we'd like to help you double-check."

4. **"It's just temporary, they'll pay me back as soon as their account is unlocked."**

What's really happening: The criminal has shown the victim a fake bank screen/website or claimed their account is frozen.

Disruptive response:

- "Criminals often use fake screenshots or fake bank links to convince people of this exact scenario. We've seen it many times. Can we help verify where this message really came from?"

5. **"They sent me ID and video calls, it's definitely them."**

What's really happening: The ID is fake or stolen. Videos may be deepfaked or manipulated.

Disruptive response:

- "Criminals are now using advanced technology to create convincing fake IDs and even video calls. Even if it looks real, we know how easy it is for these to look legitimate."

Coached Statements continued

6. **"They're in the military/working on an oil rig/doctor abroad, they can't access their money."**

What's really happening: Common cover story to avoid in-person meetings and create distance.

Disruptive response:

- "We see many criminals use these professions to explain why they can't meet or access funds. If you've never met in person, that's something to explore before making any transfers."

7. **"I don't need to explain what I do with my money."**

What's really happening: Victim has internalised shame and fear of judgment, possibly from a previously failed attempt to get help.

Disruptive response:

- "You're absolutely in control of your finances. Our only aim is to protect you from what we're trained to recognise as patterns of emotional abuse. If there's any part of you that's unsure, we're here, no judgment."

Key Patterns to Watch For:

- Defensiveness when questioned
- Statements involving secrecy, urgency, or emotional reward
- Mentions of international partners, sudden windfalls, or inheritance
- Customers appearing isolated or reluctant to talk in private spaces

Key Transaction Red Flags

Romance fraud is rarely immediate. Grooming and emotional manipulation can take weeks, months, even years, before the first financial request is made. As a result, victims often appear emotionally committed and confident in their decisions when finally initiating transfers.
Fraud teams must understand that suspicious activity in romance fraud may not always look aggressive or panicked. Instead, it can be structured, polite, and seemingly coherent, until you look deeper.

Transaction Red Flags: What to Watch For

Rounded Payments (e.g., £100, £250, £500)

- Often connected to gift card purchases, digital vouchers, or money laundering setups.
- May involve vague payment references such as “support,” “loan,” “love,” or “for family.”
- Watch for repeat purchases on the same or across multiple days or platforms.

Multiple Small or Medium Transfers in Short Timeframes

- Victims may send several payments of £200–£1,000 to avoid detection or due to scammer coaching.
- These can occur daily or weekly and often increase in urgency.
- The recipient names may frequently change, mimicking a network of mule accounts.

International Transfers to High-Risk Countries or Region-Linked Names

- Includes transfers to countries known for organised romance fraud rings (e.g., Nigeria, Ghana, Russia, Turkey, UAE, some Southeast Asian countries).
- Names may include regional linguistic identifiers, surnames, or business names not linked to the customer’s history.
- Customers may claim these are for urgent medical needs, legal costs, or to assist a partner stuck abroad.

Key Transaction Red Flags

Transfers to Domestic Accounts with Fraud Network Links

- Romance fraud has increasingly moved to using UK-based money mules.
- Transfers may go to individuals with no relationship to the victim's known contacts.
- Watch for names and reference terms matching other flagged accounts in your internal network.
- These domestic transfers may be to:
  - Businesses with untraceable service descriptions
  - Individuals with inconsistent transaction histories

Use of Cash Remittance Services (e.g., Western Union, MoneyGram)

- Often used early in the scam to "test" the victim's willingness to send money
- May precede bank transfers
- Common in multi-layer laundering or when scammers want untraceable cash

Large or Unusual Cash Withdrawals

- Especially from:
  - Older adults unfamiliar with large online transactions
  - First-time users initiating uncharacteristic branch activity

- Victims may say they're helping someone or investing in a business/purchase for a partner

Payments to Crypto Platforms or P2P Trading Services

- Victims may be asked to invest on behalf of a partner or store money in crypto wallets
- Watch for:
  - Sudden activity from previously dormant accounts
  - First-time crypto purchases by older users
  - High-volume conversions of fiat (traditional currency) to BTC/ETH/XRP etc.

Red Flag: Transactions Outside Customer Profile

Definition:
A customer profile deviation occurs when a transaction is significantly different from a customer's usual financial behaviour, based on factors such as age, transaction history, financial literacy, and known interests or investments.

Example:
A 78-year-old customer with no previous history of cryptocurrency investment suddenly initiates multiple or high-value transfers to a cryptocurrency exchange.

Why It Matters:

- This activity is inconsistent with the customer's established profile.
- Older customers may be more vulnerable to high-pressure sales tactics, online scams, or coercion.
- Banks have a regulatory obligation under KYC (Know Your Customer) and AML (Anti-Money Laundering) rules to monitor for unusual or suspicious activity.

Recommended Bank Actions:

- Flag & Pause the transaction pending further review.
- Contact the customer directly using an out-of-band method (e.g., phone call, not in-app message) to confirm legitimacy.
- Ask contextual questions about the purpose of the payment and source of funds.
- Assess vulnerability – consider age, financial experience, and potential exposure to fraud.
- Document and escalate to the fraud-prevention or compliance team before releasing funds.

Key Principle:

Uncharacteristic transactions, especially those involving high-risk assets like cryptocurrency, should not be processed without enhanced due diligence, particularly for vulnerable or elderly customers.

Important Context for Fraud Analysts

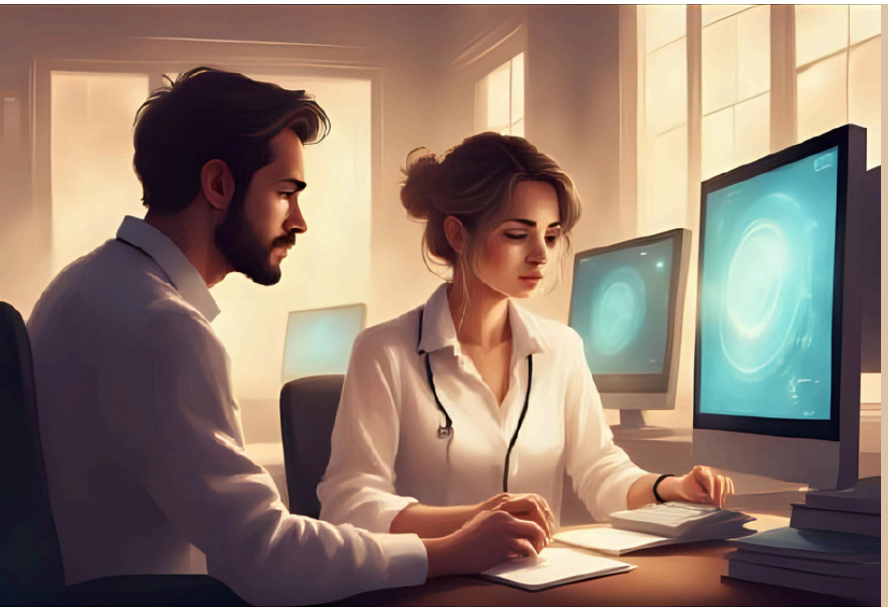
- Victims are often coached on how to respond to bank questions.
- The story may sound rehearsed and consistent, because it's meant to.
- Emotional grooming leads victims to trust the scammer more than the bank.

Summary:

Fraudulent payments connected to romance scams often follow unusual patterns:

- Rounded payments-indicating gift card purchases (e.g., £100, £250, £500)
- Multiple small or medium transfers over a short time frame
- Transfers to known high-risk countries or accounts with names linked to high-risk regions
- Transfers to in-country accounts with ethnic or linguistic links to scam hotspots (used for local laundering)
- Payments to crypto platforms or peer-to-peer trading services
- Large cash withdrawals (especially from older or first-time online banking users)
- Money transfers via Western Union, MoneyGram, or remittance services

Remember: Any payments outside of the usual, monthly spending patterns of a customer should be a trigger to look deeper.

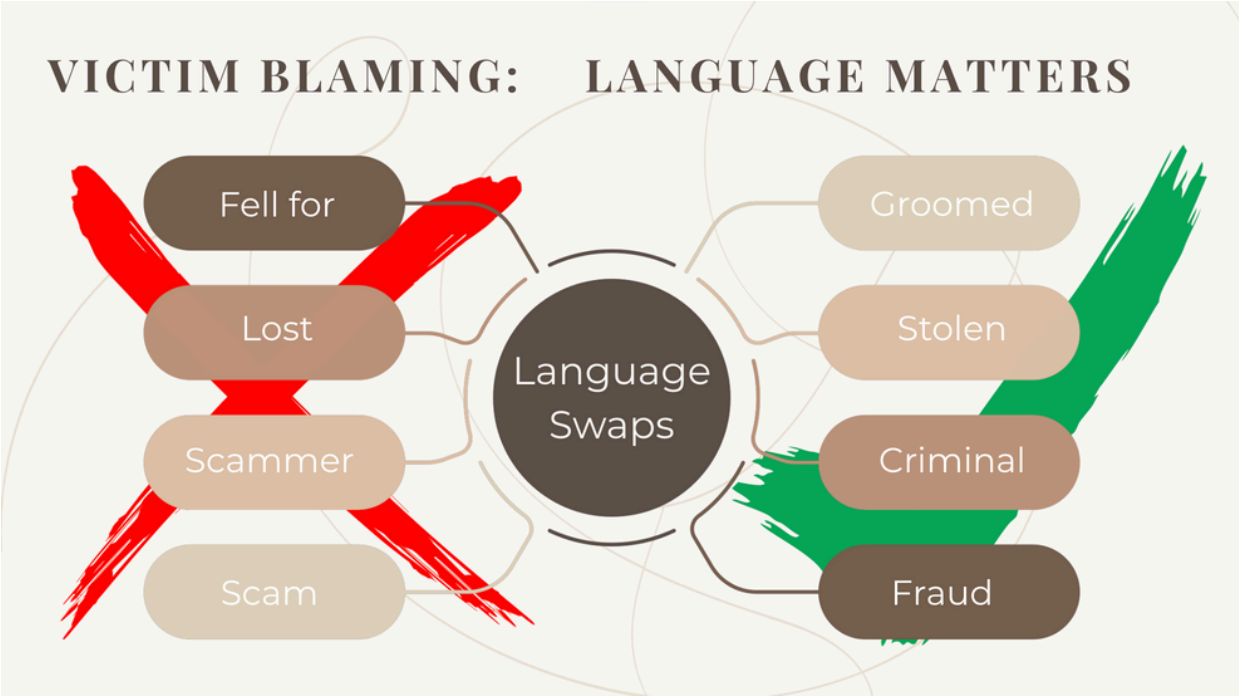


Responding with Empathy

The worst thing a bank can do is shame a victim. Survivors report that being disbelieved or blamed by their bank adds a second layer of trauma - secondary victimisation.

Train frontline staff to:

- Ask gentle but probing questions
- Understand that resistance is part of emotional manipulation
- Avoid judgmental language
- Offer time and private spaces
- Refer to a specialist team trained in romance fraud cases



Scripts for Supportive Intervention

- "You haven't done anything wrong. These frauds are designed to feel real."
- "The way this person has spoken to you, it's something we see in many victims who were deeply manipulated."
- "Smart, educated people are victims of these frauds. Your instincts brought you here. Let's honour that and double-check."

Interventions to Disrupt Fraud

Built-In Payment Warnings: Insert video pop-ups before transactions that read:

- A range of victim recorded soundbites explaining common tactics, followed by: “Would you like to speak to a specialist fraud advisor first?"

Internal Flagging System: Flag accounts with:

- Multiple crypto transactions
- Gift card (rounded number) purchases
- Overseas remittance requests from first-time users

Positive Disruption Tactics:

- Classify as temporarily vulnerable (they are being psychologically abused) to delay high-risk payments for 24–48 hours and notify the customer with a call from a trained fraud advisor
- Send printed warnings via post to older or at-risk customers
- Use empathetic AI or manual checks to spot scripts and keywords common to romance scams

Victim-Focused Recovery Pathways:

- Streamlined claims support with trauma-informed staff
- Access to specialist fraud counselling referrals
- Internal non-judgment policy for suspected fraud victims

Final Words:

- Romance fraud victims are not reckless. They are targeted and traumatised. Banks that treat them with empathy, vigilance, and responsibility become part of the solution, not just another place where the shame continues.
- Empower your teams. Spot the patterns. Interrupt the abuse.

LET'S WORK
TOGETHER

Working together with LoveSaid offers valuable opportunities for collaboration with a victim-centred organisation that prioritises empathy, safety, and recovery. By sharing best practices, insights, and resources, organisations can not only improve outcomes for victims of romance fraud but also enhance their own support services and credibility. Partnership with LoveSaid ensures that interventions are trauma-informed and ethically grounded, fostering trust and consistency across the sector. Ultimately, this kind of collaboration strengthens our collective impact in protecting and empowering those affected by online fraud.

Email:

post@lovesaid.org

Web Site :

www.lovesaid.org

LOVESAID
FRAUD CENTRE & THINK TANK