LOVESAID

2025

WHAT SOCIAL PLATFORMS NEED TO KNOW

ROMANCE FRAUD

A Guide for Social Media and Dating Platforms:
Detection, Empathy & Disruption

Prevent. Support. Empower.

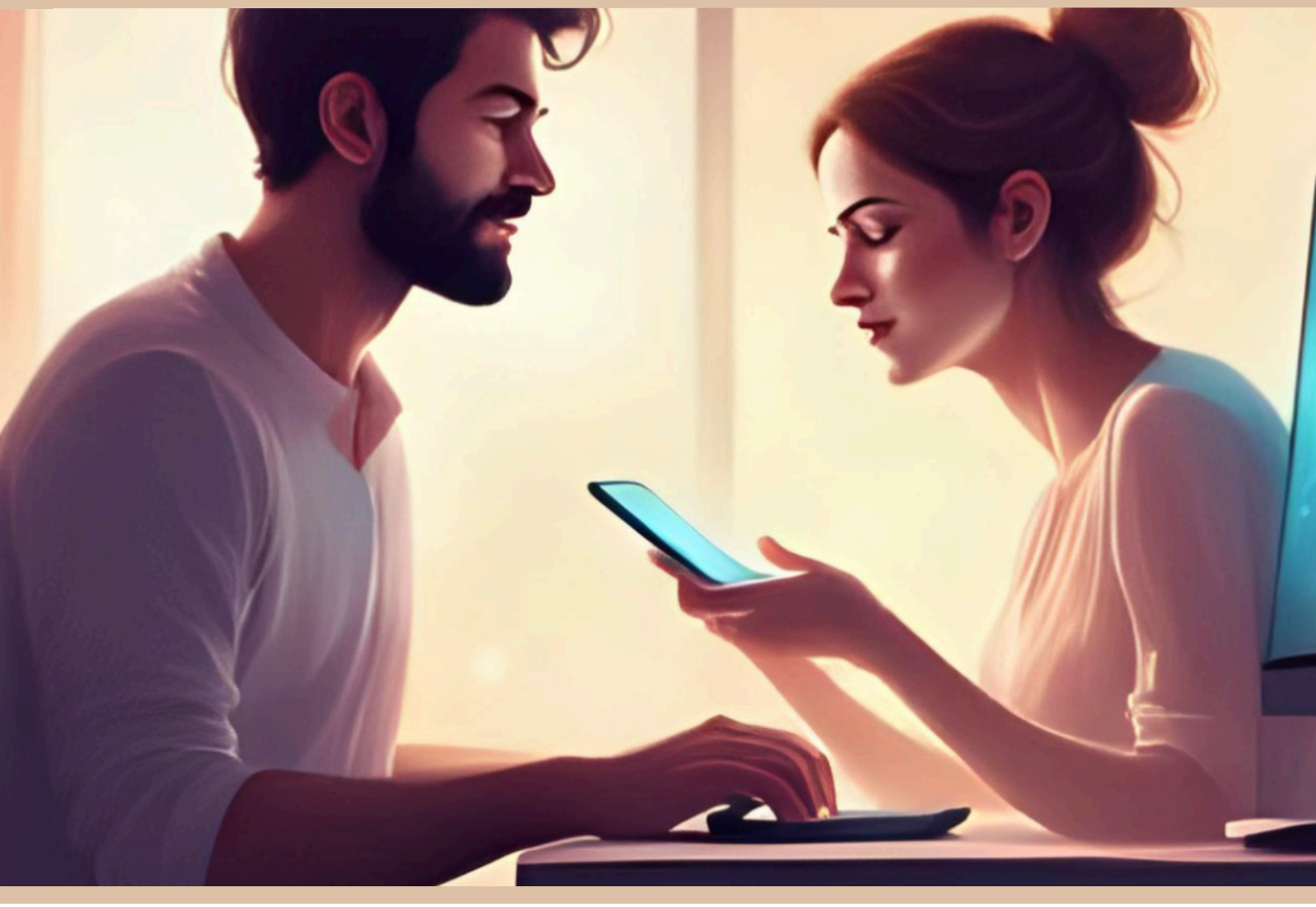


TABLE OF CONTENTS

MESSAGES FROM VICTIMS

I reported the fake profile multiple times, but they [the platform] said they couldn't find any evidence of it being fake and didn't take it down.

They [the platform] wont let me provide more evidence, even though the user was clearly using someone else's photos and had a suspicious profile,"

"I lost a significant amount of money to a romance scammer on this platform, and when I reported it, the auto system just told me to contact the authorities. They did nothing to help prevent future scams.

After I discovered I was being catfished, the platform deactivated my account instead of the fake one, making it harder to gather evidence and report the scammer.

I was targeted with explicit images and messages, but the platform took no action after I reported them. I felt incredibly unsafe and unsupported.

The platform made it incredibly difficult to report the scammer, and when I finally did, they didn't seem to take it seriously. I was left feeling vulnerable and ignored,"

I was bombarded with messages from a fake profile, and when I tried to block the user, they just created new ones. The platform didn't seem to have any effective measures to stop this.

These are just a few examples of the widespread dissatisfaction with platform support regarding fraud and catfishing. Many users feel that the platforms prioritise their own profits over the safety.

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 platforms sit at the start of the abuse and the pending financial harm.

Platforms are where this starts. With the right awareness and tools, you can become a critical line of defence.

Romance fraud is not a fringe issue. It is a growing, organised, and psychologically complex crime that moves billions globally, and platforms sit at the start of the abuse and the pending financial harm, alongside other crimes.

Platforms are where this starts. With the right awareness and tools, you can become a critical line of defence.

Recognising Signals and Markers

If it is already there-remove the profile, remove the harm

Romance fraud and online scams are increasingly being conducted via fraudulent social media profiles. Fraudsters create fake personas to build trust, manipulate victims emotionally, and exploit them financially or personally. Unlike dating platforms, where users actively seek relationships, social media platforms facilitate broader interactions, making them a prime target for criminals and unsuspecting targets.

Recognising Fraudulent Profiles: Social Media & Dating Platforms

Most platform users reporting fraudulent profiles do not have access to human support, as many platforms rely on automated systems. This toolkit provides guidance on effective automated and human responses, helping to ensure that victims are supported and fraudulent activity is addressed. Criminals on social media often use extra tactics that differ slightly from those on dating apps. Common signs include (and many are being ignored):

High Risk:

- **Newly created** or sparsely populated accounts – Few posts (or many loaded on the same day), little engagement, and/or a sudden influx of friends/followers (bought).
- **Stolen images** or AI-generated profile pictures – Reverse image searches may reveal duplicate photos. AI facial recognition when onboarding could end the use of stolen photos.
- **Fake celebrity or influencer** impersonation – Claiming to be a well-known figure engaging personally with users (including 'fan pages').
- **Unrealistic interactions** – Rapidly forming connections with multiple users and high volume of messages with same script.
- **Requests to move conversations off-platform** – Encouraging users to switch to private messaging apps.
- **Investment advice or financial talk on profiles** – Setting the scene for fraud.
- **Financial requests** – Claiming they need money for an emergency or promoting 'too good to be true' investment opportunities.

These requests are unlikely to happen on your platform.

Recognising Signals and Markers

Remove the profile, remove the harm

Other things to consider:

Common Language Red Flags

Watch for repeated phrases and emotionally loaded terms that criminals often use to build trust quickly:

- "Widowed" or "recently widowed"
- "God fearing" or overly religious language early on
- "Looking for serious relationship only"
- "I don't want to play games"
- "I believe in love at first sight"
- "Destiny brought us together"

These phrases are often part of the profile as well as a grooming script designed to fast-track empathy and intimacy.

Professions Often Used by Scammers

Criminals frequently claim to be in jobs that involve travel, isolation, or prestige. Be especially cautious if someone claims to be:

- Military personnel (deployed or peacekeeping missions)
- Oil rig or offshore workers
- Engineers, architects or contractors working abroad
- Pilots or captains, including with international aid agencies or military
- Surgeons or doctors, including with international aid agencies or military
- UN peacekeepers or contract consultants
- Celebrities
- Luxury goods dealers
- Widowed fathers or single parents overseas

These roles are chosen to explain why they can't meet in person, have inconsistent internet access, or need financial help.

Recognising Signals and Markers

Remove the profile, remove the harm

Red Flags in Photos & Profiles

- Photos can look staged, filtered, or too professional
- Reverse image search shows them on stock photo sites or used in multiple profiles
- All photos might be uploaded on the same day
- Follows only or mainly one gender (usually their target)
- No tagged photos, from family members or family in friends list
- No comments or engagement from real friends or family
- Tagged photos can show an old owner of the profile
- Links to African profiles which seem outside the photo's demographic
- Profile is new or has few connections
- Uses two first names
- Check user names and links-sometimes these are mismatched when profiles are being recycled or have been hacked
- Check his/her (changed his/her/their profile picture) matching profile gender, on posts (Facebook) can be mismatched
- Grammar and spelling can be off

Automated Responses for Fraud Reports

When a victim reports a fraudulent profile, automated responses should be:

Acknowledging the report:

"Thank you for reporting this account. We take user safety seriously and will review the profile as soon as possible."

Encouraging additional safety measures:

"We recommend blocking the reported account and avoiding further communication. If the account asked for money or personal information, consider reporting it to law enforcement."

Providing external support resources:

"If you believe you have been targeted by fraud, you are not alone. You can seek guidance from trusted fraud prevention organisations such as [Insert Relevant Organisation]."

Avoid dismissive or unclear automated responses like:

"This does not violate our community guidelines." (Instead, clarify why and how users can provide additional evidence.)

When a victim knows this is a fraudulent profile (as well as the many others they may see with the same pictures that are not the real one) it is incredibly re-traumatising knowing these are harming others in the same way.

Human Support for Escalated Cases

Some fraud reports require human intervention, especially when:

- The victim has lost money or shared sensitive information.
- The reported profile is part of a larger scam network.
- The victim is experiencing distress, harassment, or ongoing manipulation.

DO say:

- "We understand how distressing this experience can be. You are not alone, and we want to support you."
- "Scammers use sophisticated techniques, including stolen identities and AI-generated content, to make their accounts appear real."
- "We have removed the reported profile and will continue monitoring for similar activity. Please let us know if you encounter any further concerns."
- "Would you like us to provide additional safety resources or guidance on next steps?"

AVOID saying:

- "Why did you interact with them?"
- "There's nothing else we can do."
- "This happens a lot; you should be more careful."

Supporting Victims Post-Fraud

After confirming a fraudulent profile, social media platforms should:

- Remove **and** flag the account – Remove it **and** investigate related accounts. Anyone that is still following the fraudulent account that has been messaged (or those who may have been blocked (scammer trick to make the victim believe they left the platform) , should be notified it was a criminal so that any who have moved off the platform to communicate (highly likely) are warned to cease the communication.

- Provide victims with safety resources – Share fraud prevention tips and links to other agencies.

- Encourage reporting to authorities – Guide victims on how to report the fraud outside the platform to their relevant authorities and banks.

- Offer additional security options – Suggest enabling two-factor authentication and reviewing privacy settings.

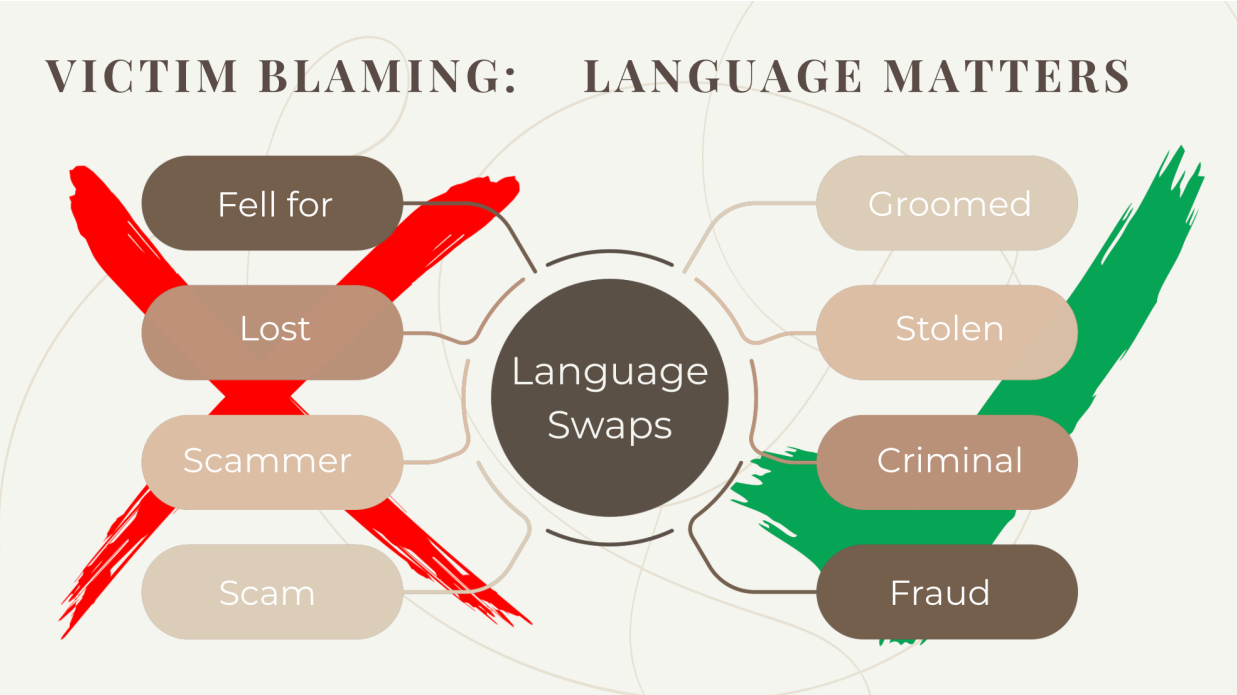
- Share the data from the profile with authorities and other platforms so that they can block the IP's, numbers and emails.

Responding with Empathy

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

Train 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."

Strengthening Platform Safety Measures

As a minimum

Social media and dating platfoms can enhance fraud prevention by:

- Improving verification systems – Encouraging ID verification for high fraud-risk area profiles, or those using a VPN.
- AI-driven scam detection – Identifying and removing fraudulent activity faster. AI should be used for facial recognition with photos to automatically remove multiple profiles using the same face, especially where the legitimate user is verified.
- User education – Posting ***regular*** fraud and scam awareness content.
- Transparent reporting processes and account information – Making it clear how reports are handled, currently every platform is sporadic and nonsensical.
- Investing in human review teams – Ensuring critical cases receive human oversight.

In depth

Dating platforms and social media play a valuable role in helping people build meaningful connections, fostering relationships across distances and cultures. As these platforms grow in popularity, maintaining user trust and safety is not only a moral and ethical responsibility, it's essential for long-term success. Prioritising a secure, respectful user experience builds loyalty and protects the integrity of the platform. The proactive and reactive measures outlined here offer practical steps to identify and reduce fraudulent profiles, ensuring users feel confident, protected, and valued.

During Onboarding

- Identity Verification: Suggestions can be-Require government-issued ID, phone number, or social media account linkage to confirm user identity. Email/Phone Validation: Send verification codes to ensure the email or phone number is active and belongs to the user (hacked accounts can be altered).
- Cross-Platform Intelligence Sharing: Scammer Intelligence Networks – Collaborating with other platforms, financial institutions, and cybersecurity groups to flag shared scam profiles, behaviour patterns/repeat offenders.
- Collaboration with other dating platforms could use a data base for checks. Blockchain-Based Identity Verification: Use decentralised identity systems to create tamper-proof user credentials, reducing anonymity for fraudsters.
- Profile Photo Analysis: Use reverse image search to detect stolen or stock images commonly used in fake profiles.
- IP Address Tracking: Flag accounts created from suspicious IP addresses, such as those linked to VPNs or known fraud hotspots.
- Geolocation Anomalies: Flag profiles where location data (e.g., GPS, IP) mismatches claimed location or shows rapid, implausible changes.Behavioural Checks: Monitor for rapid profile creation, incomplete profiles, or generic responses that suggest automated bot/copy & paste activity.
- Machine Learning Filters: Deploy algorithms to detect patterns in profile data (e.g., repetitive text, unrealistic bios) indicative of fraud.
- Device Fingerprinting – Helps detect multiple accounts created from the same device
- Facial Recognition with Liveness Detection: Require video selfies with real-time movement (e.g., blinking, smiling) to verify that profile photos match the user and aren't manipulated.

Post-Onboarding (Ongoing Monitoring and Member reports)

- AI-Powered Behavioural Analysis: Use advanced AI to analyse user interactions (e.g., typing speed, message patterns, or response times) to differentiate human users from bots or scammers.
- Natural Language Processing (NLP): Detect scripted or unnatural language in messages, such as phrases commonly used by scammers or romance fraud templates.
- Geolocation IP's: Flag profiles where location data (e.g., GPS, IP) is changing (could be VPN use)
- Dynamic Risk Scoring: Assign real-time risk scores to profiles based on behaviour, updating scores as new data, profile changes (hacked accounts) e.g., reports, interactions) emerges.
- Automated Shadow banning: Quietly restrict suspected fake profiles' visibility or messaging capabilities while investigations occur, minimizing user disruption.
- Crowdsourced Moderation: Allow trusted users to participate in flagging suspicious activity, with rewards for accurate reports, creating a community-driven moderation layer.

New Innovative Approaches

- User Reporting Systems: Allow users to flag profiles for suspicious behaviour, with clear reporting options like "fake profile" or "scammer." allow space for uploading a real persons profile or messages off platform where there is the money ask.
- Manual Review: Employ moderation teams to investigate reported profiles, cross-referencing reported data with platform activity.
- Suspension/Ban Protocols: Temporarily suspend or permanently ban profiles confirmed as fake, preventing further interaction-linked to alerting users.
- Pattern Analysis: Aggregate reports to identify trends, such as multiple reports targeting similar profiles or behaviours.
- Communication Monitoring: Review reported conversations for red flags like financial requests, inconsistent stories, or scripted messages.

Alerting Users

- InApp Fraud Alerts: Send discreet notifications to users if they've interacted with a profile flagged as suspicious, e.g., "This profile has been reported; proceed with caution as we are monitoring."
- Scam Pattern Education: Push micro-tutorials or pop-ups warning users about common scam tactics (e.g., requests for money, overly quick emotional bonding).
- Real-Time Interaction Warnings: Use AI to monitor chats and alert users mid-conversation if red flags appear, like links to external sites
- Personalised Risk Notifications: Inform users if their behaviour (e.g., frequent engagement with risky profiles) suggests vulnerability to scams, offering tailored safety tips.
- Post-Interaction Feedback Loops: After a conversation ends, prompt users to rate the interaction's authenticity, using responses to refine fraud detection algorithms.

Proactive Member Safety Features

- Scam Interaction Alerts – If a reported scammer engaged, interacted with other users, including off platform, those users receive a discreet message like: "A profile you recently engaged with was found to be in violation of our safety standards. Please review any conversations or actions you may have taken and report anything concerning."

- Trust Scores or Badges – An evolving, AI-driven "trust rating" for users (similar to Uber's rider/driver scores), factoring in verified identity, behavioural patterns, and reporting history.

- Community-Based Review Panels – A pool of trained volunteer moderators from the platform's user base to review questionable profiles for transparency and democratic moderation.

These approaches reflect a necessary evolution in safety standards for dating and social media platforms in response to the increasing sophistication of online fraud. By combining smart onboarding, continuous monitoring, AI detection, and user empowerment, platforms can dramatically reduce the risk of romance fraud while preserving trust and experience.

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