Romantic Scam: "My Partner Might Be a Scammer" #1

Client Type: Everyday person
Problem:

"I met someone online. We've been talking for months. They say they live in another state, have some money problems, and need help getting back on their feet. I've already sent $1,800. I don't know if I'm being scammed, or if they're just struggling. Can you find out the truth?"

Step 1: Intake Questions (Fast Client Form)

- How long have you known them?
- Have you spoken on the phone or video?
- Have they ever refused to meet? What's the reason?
- What details do you know about them? (Name, alias, email, phone, location, etc.)
- What have they asked for (money, favors, accounts)?
- Do you have any screenshots, voicemails, payment history?

Step 2: Core Collection Moves

Objective	Tactic	Tool
Confirm identity exists	Public records, obits, Pipl, BeenVerified, Whitepages	People-search & records tools
Check for scam behavior	Image reverse search (Tineye, Yandex), username reuse, romantic scam keywords	Open source tools
Spot digital inconsistency	Metadata from photos or emails, time zone slippage, language mismatch	Exif viewer, WHOIS
Look for networks/fake personas	Social circle inconsistency, cloned accounts, reused bios	Facebook, LinkedIn, Twitter deep dives

Objective	Tactic	Tool
See if they're already reported	Scamwatch, Reddit, forums, BBB, legal filings	OSINT + reputation sites

Step 3: Final Product – 1-Page "Risk Summary"

Online Relationship Briefing – "Reality Check"

Client ID: 2024-138
Subject: "Jay L." from Houston, TX
Summary Verdict: ⚠️ Likely Fraudulent Relationship

Key Findings:

- Subject uses a name tied to 4 scam reports in 3 states
- No verifiable employment, residence, or family connections
- Phone number linked to VOIP burner; not local to Houston
- Money request pattern matches standard romantic scam model
- Repeated postponement of meeting, no video proof

Recommendations:

- Cease financial contact
- Consider filing with IC3.gov (FBI)
- Monitor for recontact using alternate aliases (provided in appendix)

Risk Indicators Table

Behavior	Confidence	Notes
Refuses video chat	🔴 High	6 excuses in text logs
Uses VOIP number	🟠 Medium	Number used in 3 scam reports

Behavior	Confidence	Notes
Sends same selfie repeatedly	🔴 High	Tineye shows image posted in 2022 elsewhere

Mini-SAT: Key Assumptions Check

✅ “We assumed the person texting was the person in the profile.”
🔴 This broke: phone is a VOIP burner & tied to other aliases.

✅ “We assumed their story about location and job was real.”
🟠 Inconsistent — no property, license, or employment found.

✅ “We assumed they were motivated by connection.”
🔴 All money requests followed emotional hooks & escalating crises.

Suggested Package:

- Add-on: 20-minute call consult +$150
- Optional “Watch List” follow-up: +$100 in 3 months
- Full Date Archive as a zip file or on a secure drive (for +$50–100)