True love scams that never die

***Charanjeet Singh** highlights some online dating scams and explains how mobile banking apps can be improved to give greater protection for users against such fraudsters*

When Thomas's wife passed away after a marriage of 35 years, he felt lonely and started to spend his time surfing the web. He already had accounts on Facebook and Instagram, but now he also set up an account on a dating website for seniors. He was particularly drawn to one of the women he 'met' there. Leena was witty, always replied promptly no matter what time he sent her a message and treated him with respect. They would spend hours chatting and sharing details about each other's life. Suddenly, Thomas started to feel happy and optimistic again. He felt he was falling in love.

Leena told him that she was 10 years younger, divorced and responsible for her elderly father as well as herself. She was so happy to find a soulmate such as Thomas after all she'd been through. It would be wonderful to meet, but she was

> *"Romance scams are frauds that rely on exploiting trust and our need for emotional connection*

too short of money to travel to the other side of the world. Thomas gallantly offered to buy her ticket. Leena said no, she didn't want to burden him. It was too expensive. Thomas insisted. Alright, Leena said, but she had an idea that would save Thomas money. If he sent the funds direct to her father's account, she would buy a cheaper ticket with that. Thomas quickly transferred £2,000. Leena was thrilled, but then found that she needed to renew her passport and doing that quickly would be expensive. She offered to return the money for the ticket, but Thomas wouldn't hear of it. It would be his pleasure to send a further £1,500 so Leena could get a new passport made quickly.

Yes, as you would expect, this is a tale of yet another 'romance' scam. Not only can the people targeted lose large amounts of money, they can be left broken emotionally. Romance scams are an example of social engineering fraud that relies on exploiting trust and our need for emotional connection. Variants include getting people to transfer funds for buying a pet, asking them to help the 'police' to catch thieves by sending money (guess who controls the account), and suggesting that, by making advance payment on taxes, they'll receive an inheritance from a distant, rich, unknown relative.

Social engineering scams are very effective. According to the FBI, about 24,000 victims in the US reported losing a total of around $1bn to romance scams in 2021. The FBI says that figure is almost certainly a significant undercount because many victims are too ashamed to report the scam. Estimates suggest that more than one-third of the money lost comes from older adults aged between 55 and 64.

Many organisations, including government agencies, are raising awareness and sharing tips on how to identify and protect against romance scams. These laudable campaigns, however, all share a major weakness: they expect potential victims to protect themselves. But the reason fraudsters are able to charm their way into the wallets of their victims is that they target the one thing that no one can change: being human. So, what if, rather than relying on victims' ability to protect themselves, we could leverage the objectivity of technology to offer another layer of protection?

Should banks be held responsible?

Scammers need victims to send the funds via banking channels or money transfer services. When the victim realises they've been defrauded, they turn to those banks or transfer services to get the money back.

The problem for the financial services firms is that the customer willingly pressed 'send', sometimes overriding warning messages. That's like taking cash out of a purse and handing it over. Customers are often horrified to discover that banks don't have to refund them.

That refusal to refund isn't just because banks can't, and shouldn't, control what customers do with their money. It's also because paying back customers when they say they've been scammed would leave the bank open to fraud – including fraud by customers.

But financial services firms can help protect customers' money. Banks can block payments if the customer requests that quickly enough. With scams, though, sending recall messages is usually futile. Fraudsters don't leave the stolen money sitting in the account. They immediately transfer it through a network.

The more powerful approach that banks can offer is to

encourage customers to think carefully about who they are sending money to and why. They could, for example, list "payment being sent to support someone I have never met", or "payment being sent based on email/phone call/sms" as purpose of payment.

Suspicious payments could be put on hold until a member of the bank's staff securely contacts the customer to obtain more background on the payment. How would the customer know they're talking to their bank? In the United Arab Emirates, the telecom regulator requires banks (and other firms) to take part in a secure caller ID system that protects against spoof calls. It would also be possible to build a secure service into a banking app.

In some cases, the customer could be asked to go to a branch to talk to trained staff before making the payment. Over time, artificial intelligence and machine learning will automate such calls and payment processing.

In principle, a tech integrator could connect the mobile banking app with the dating app. That could then use some of the tools below to protect against romance scams.

• **Digital identity.** Anyone can create any online persona or username. As they say, when online nobody knows you're a dog. But although people might not know they're dealing with a golden retriever, they can know Rover's digital pawprint. That's a combination of IP address, device ID and email ID, among other things. Taken together, such data points create a unique digital identity. If one digital identity includes, say, data from different devices or IP addresses, suggesting that more than one person is involved in creating and maintaining it, it could be tagged as potentially dangerous.

• **Common credentials.** Is the unusually attractive person you think you're messaging really who you're talking to? Online images can be reverse-searched to find out. That will show whether what you're looking at is really the picture of another person on a different website, or a stock image. An example could be Leena who claims to be living in Turkey, but her profile picture matches with Maria, who is living in Romania, according to her Facebook profile. That doesn't tell you whether Maria really exists, but you do know more about Leena.

• **Geolocation.** The wonderful new person you've found on the dating site tells you they are in Turkey. Are they really? A tech integrator could use an IP address to give an approximate location of the profile. If the purported location of the 'friend' is different from the real location, the consumer could be alerted.

• **Standard texts.** Are you chatting to a new friend, or to a standardised scam? Scammers have a good understanding of psychology and have developed standard texts that make it easier for them to 'work' on many targets at the same time. If such standard replies and approaches are being used by different profiles, that can indicate either a bot or the same person behind different profiles. Key words such as 'need', 'money', 'transfer', etc could flag potential scams.

> *Online images of the beautiful person you are talking to can be reverse-searched to check if that respondent is genuine*

• **Verified profiles.** Users who take video selfies and upload identity documents get a 'verified' profile. That provides assurance to others that they are dealing with a real person and not a synthetic profile. The tech integrator could verify the documents using genuine samples and validate that the image on the documents and video selfie are of the same person.

• **Digital fraud protection services.** Digital fraud protection could come preinstalled by the tech integrator as part of mobile banking apps, social media apps and cryptocurrency wallets and could be offered free to seniors. Others could be charged for the service. It could also be used by businesses to protect them against frauds such as Business Email Compromise (BEC/redirection fraud).

What dating websites can do

In principle, offering digital fraud protection on dating websites should attract more users. People could be sure that the person they're in contact with really is who they claim to be.

Many legitimate sites already do offer protection to clients, such as messaging apps that track all interactions. But there are also dating sites set up to scam and they may look more tempting. After all, most people aren't very glamorous or rich. If you find you're suddenly dealing with many wonderful online dating prospects, remember: if it's too good to be true, it's probably a scam. ■

(These are the personal views of the author and do not represent the views of his previous and/or current employers.)

***Charanjeet Singh** is Head of Fraud Risk at a large bank in the UAE*