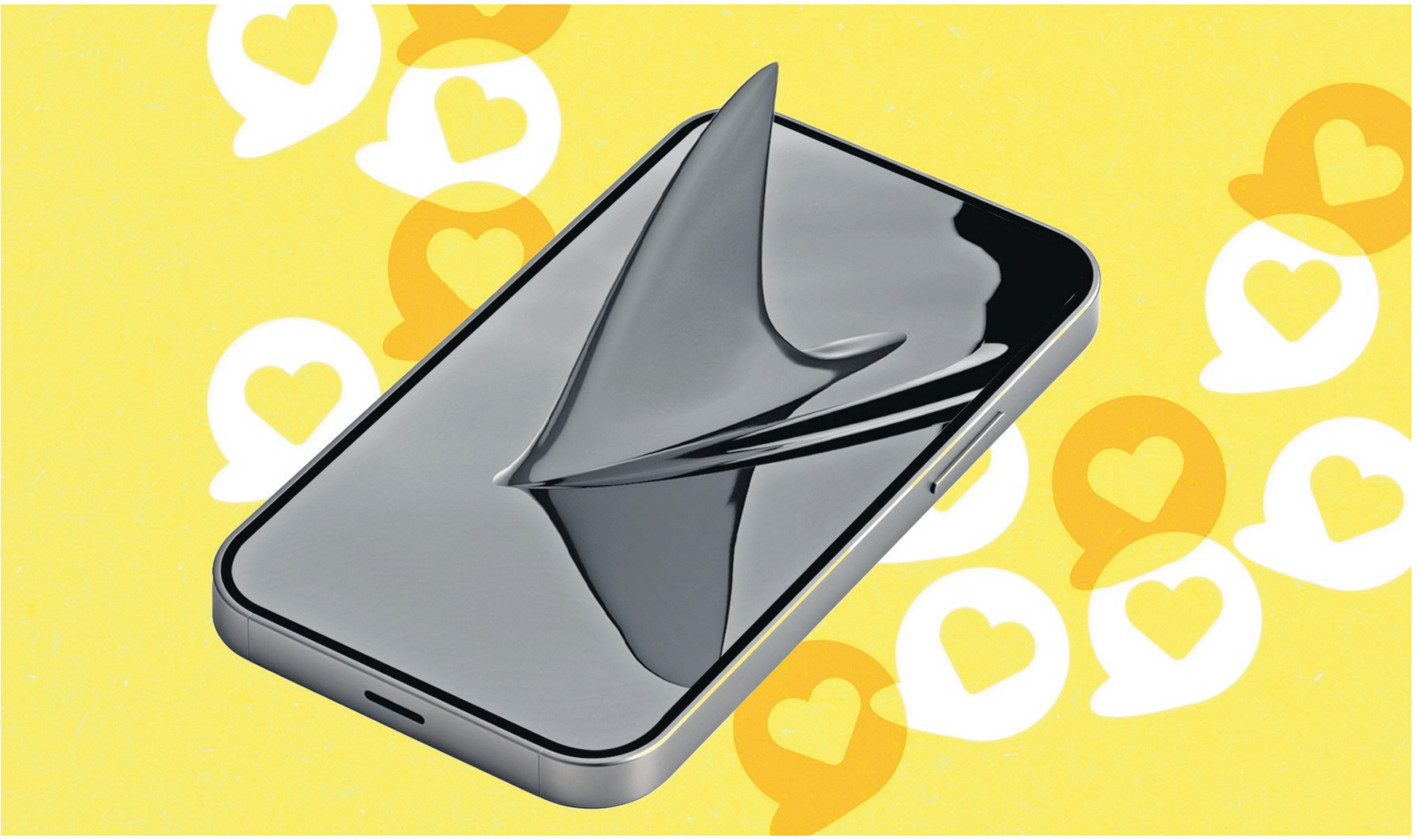
WeekendFin

www.afr.com | 4-5 July 2026 The Well-Lived Life

Edited by Emma Connors: emma.connors@afr.com

Smile to frown
Lily Allen defends 50-minute show
p40

Lunch
Ex-WA premier Colin Barnett on Xi and billionaires
p41



WHEN SWIPING'S NOT RIGHT

Online dating Last year the face of 'Steve, 53' turned up on Bumble. The world knows him as Hamish McLaren, a criminal who conned 15 Australian women out of more than $7.6 million, writes **Tracy Hall**.

There is a particular kind of dread that comes not from the unknown, but from the all too familiar. In July 2025, I discovered a profile on Bumble that turned my blood cold.

A profile with the image of Hamish McLaren – an incarcerated criminal – now presenting as "Steve, 53". A verified profile accompanied by a Bumble tick of approval. A little symbol that implies in a big way "you can trust this person is who they say they are".

This profile picture was of a criminal with a history of financial harm, a history of using a false identity to access women, and a man whose pattern of behaviour had left devastation in its wake. He will be released on parole on July 10.

Real women connected with this profile, had entered real conversations and were likely planning to meet "Steve" for a real date.

Ten years ago, I met a man by the name of Max Tavita on a different dating app. He was 41. We were in an intimate relationship for 16 months.

He stole my life savings – $317,000 – and I was forced to start again financially and emotionally at 42 as a single mother. His name was not Max Tavita. He was not 41. He was, in fact, 46-year-old Hamish McLaren – one of Australia's most notorious con men.

He was arrested and eventually sentenced for defrauding 15 Australian victims of more than $7.6 million. An investigative podcast by *The Australian* revealed it was probably more than $70 million globally. A year ago, on July 6, Greg Bearup, the reporter behind that podcast, received a tip off about the profile. He passed it on to me.

When this profile of "Steve, 53" appeared on Bumble, Hamish McLaren was in jail. He was 12 months away from his parole hearing and, confirmed by authorities, not allowed access to a mobile phone.

So I reported it. What happened next will tell you everything you need to know about how dating apps respond to the safety concerns of women on their platforms.

Between July 7 to 10 last year I contacted several senior trust, safety and law enforcement executives from Bumble on LinkedIn, pointed them towards the profile and asked for help to take it down. They advised they "couldn't assist me directly" and suggested I fill in a generic webform. That was it. A webform. For one of the most documented serial con men in this country's history.

On July 10, I reluctantly filled in the form, again asking to speak to someone urgently. Over the next 10 days there was a lot of back and forth with Bumble asking me for my member details. I repeatedly told them I was not a member.

They were also seeking details of the profile in question and refused to communicate via any method other than the faceless webform, even though I repeatedly requested to speak to a human.

On July 26, Bumble's member support eventually confirmed the "Steve, 53" profile had been removed prior to my initial report on because it was "flagged by another member of our community". On July 31, Bumble stated "the account using the images of McLaren was not operated by him".

Australians lost $140 million to romance scams last year. ILLUSTRATION: BRYAN COOK

How could the company be sure of this? Do you know how easy it is to set up a fake profile on Bumble under a different name, email address and phone number? I do, because I've tested the system.

Another question I had: How and why was the profile verified with a tick if it wasn't McLaren? Photo verification is confirmed by taking a selfie in a specific pose when requested and matched to the user's profile pics.

I've asked these questions many times and been told that "moderation mistakes can happen so we have robust processes in place to identify and remediate instances of incorrectly verified or moderated accounts and content on our platform".

Frustrated, I changed tack and asked Bumble whether it intended to inform the women who connected with "Steve" they had been talking to someone impersonating a convicted criminal. It's commonplace to take conversations off-platform and communicate directly following a connection, so while the profile had been removed from Bumble, there was a chance that some women may still be communicating with him.

I'd discovered Hinge does this consistently in the UK when profiles are flagged as potentially fraudulent. While prevention is always better than cure, this was a safety feature I thought Bumble could implement as well. Bumble was vague in its response to this suggestion. "We take appropriate steps which may include notifying those affected". I'm not sure if Bumble did let anyone know. Certainly a girlfriend of mine who was chatting to "Steve" was not notified.

Bumble did, however, confirm a report was emailed to NSW's Police Corrections Intelligence Unit on July 22, 2025, though it did not hear back. The company also confirmed it had added a photo of Hamish McLaren to their database which automates blocking and prevention of new accounts being created using those images.

I can't help but wonder if they shared this database with other online dating platforms or perhaps thought about creating a centralised version?

While all of this was happening, and at a loss of how to escalate this appropriately beyond a generic webform, I reached out to the eSafety Commissioner who responded with urgency and care and reassured me the matter was being taken seriously. The office did everything it could, but the information it could provide and its remit is limited.

The global online dating industry is worth more than $US6 billion ($8.56 billion) and it's set to reach $US17 billion by 2030. About 360 million people used dating apps in 2025; interacting daily on platforms that know their age, location, attachment style, preferences and relationship history.

What the platforms do not know – and have chosen not to compulsorily require – is the official identity of who is actually on the other end of the screen. Given these companies generate billions of dollars in revenue, they cannot claim ignorance or poverty. What they can claim is that safety is the user's problem.

Bumble's own global research in 2023 revealed that respondents cited fake profiles and the risk of scams as their top concerns when online dating. Almost half of women surveyed (46 per cent) said their number one issue while dating online was not knowing if the person they're talking to was who they say they are.

A study by global identity technology business GBG found that 61 per cent of online daters in the UK have matched with fake profiles.

According to Norton's 2026 Global Insights Report, 34 per cent of current online daters have been targeted by a scam; of this group, 64 per cent have become victim to one. Financial losses in Australia averaged nearly $12,000 per victim.

He stole my life savings … I was forced to start again financially and emotionally at 42.

Tracy Hall

Tracy Hall with the man she knew as Max Tavita, who was revealed to be con-man Hamish McLaren; Hall at Freshwater Beach. PHOTO: LOUISE KENNERLEY

Romance fraud is big business, albeit grossly under-reported. Last year Australians lost $140 million to romance scams and, according to an ACCC National Anti Scam centre report, most romance scams begin on dating or social media platforms.

In the US the estimated losses were $US1.4 billion, and in the UK £102 million. In all three regions, the numbers increased year-on-year. Clearly, this is not a niche issue experienced by an unlucky few.

In March 2025, Bumble launched an ID verification feature – a government-issued ID check, developed with identity provider Veriff, available in Australia, the US, the UK, and several other markets. It sounds promising. It is, in fact, voluntary. Users may choose to ID verify on top of the standard selfie check. Or they may not. Hamish – or Steve, 53 – chose not to.

Tinder has made similar moves. Match Group, which owns Tinder, Hinge, and others, has built what it describes as shared safety infrastructure across its portfolio.

Yet across these platforms, identity verification remains optional, and the burden of proof continues to fall on the woman asking her match to please confirm they are who they say they are.

I speak to victims of romance fraud weekly and sadly the stories are all very similar. Fake profiles and fake love but very real emotional and financial devastation.

The one that haunts me is Jade – a university educated, Queensland single mother of three who met a French man by the name of Nico on Hinge in early 2025. She had $840,000 stolen in an elaborate romance baiting scam.

A safety guide and some optional features versus mandatory ID verification? I know what Jade's preference would be.

It's easy to say a victim should have known better or should have been more careful. The tools used against us are not the blunt instruments of opportunistic thieves in basements down the road. They are sophisticated weapons designed to defeat rational judgment often carried out by transnational organised crime groups.

The psychological scaffolding of romance fraud – the reciprocity, the urgency, the manufactured intimacy, the strategic exploitation of our deepest human need for connection – is engineered specifically to bypass our defences.

Telling victims they should have been more careful is like telling someone shot by a sniper that they should have ducked.

Sophisticated strategic exploitation requires a combative solution more robust than a safety guide and a selfie check. These criminals know how to weaponise tech to facilitate abuse and this is why mandatory ID verification matters.

For more than a decade, public policy in many jurisdictions relied heavily on platform self-regulation to manage identity related harms. The prevailing assumption was that market incentives, reputational pressures, and voluntary codes of conduct would be sufficient to maintain acceptable levels of safety and trust. Experience suggests limitations in this approach.

First, there is an incentive misalignment. Platforms are rewarded for growth, user acquisition and frictionless onboarding. Strong identity verification, age gating and structured enforcement mechanisms introduce friction and may reduce sign-ups or engagement metrics. Commercial incentives therefore do not consistently align with higher assurance identity controls.

When asked whether stronger and compulsory identification controls should be implemented, the platforms' responses suggest users would not accept such measures. They believe requiring identity checks would scare people away.

Surely those resistant to being identified are exactly the individuals we don't want to be exposed to in digital environments where anonymity equals high risk.

The Voluntary Online Dating Code was introduced in Australia in 2025 to address "tech facilitated violence and harm". The government has no statutory powers to enforce compliance with this code. It is, in effect, a set of promises made by the same companies whose commercial interests are served by keeping friction – and accountability – to a minimum.

The eSafety Commissioner is due to release a report assessing the effectiveness of these measures, with key indicators including account suspensions, moderation efforts, and complaint resolution rates. I await that report with interest.

After discovering the profile with Hamish's photo, I engaged with the code and its complaint process, reporting "Steve, 53" and my concerns. The code secretariat's response was to make two recommendations to Bumble.

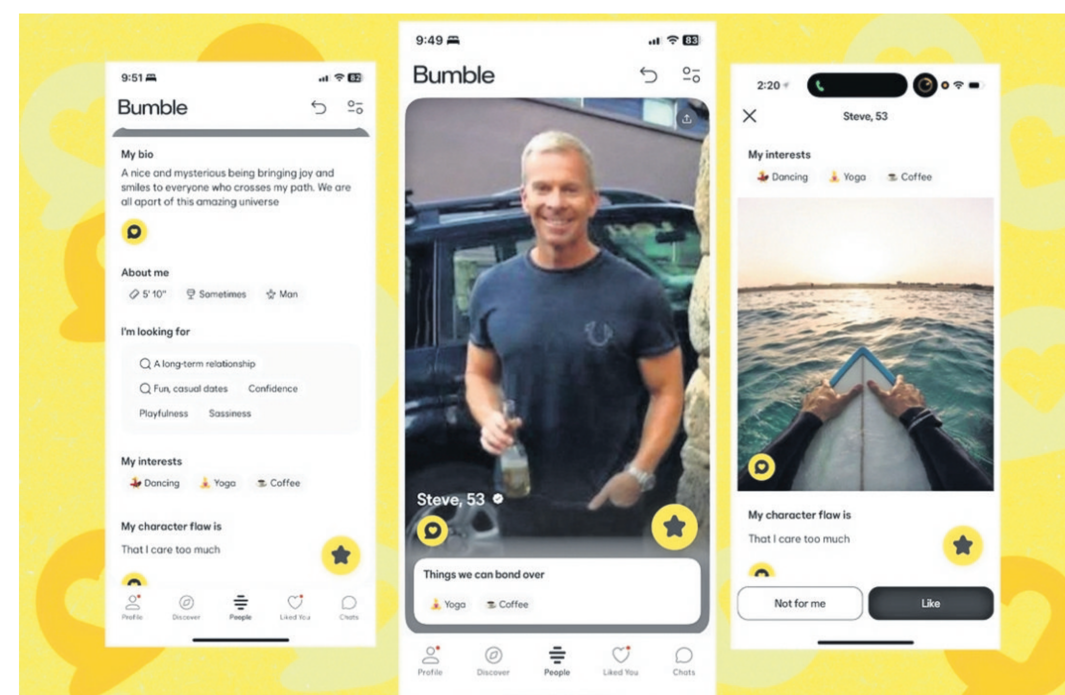
Firstly, it advised the dating app to review its internal procedures and policies to ensure that complaints, whether communicated in-app or otherwise, can be appropriately escalated and resolutions communicated to the complainant in a timely manner.

Secondly, it wanted Bumble to improve the prominence of its complaints and reports mechanism, including for non-active users of their platform – such as me.

The code could have – but didn't – recommended that Bumble share the profile with other platforms and inform users who had connected with "Steve" they were communicating with a fraudulent profile at best, a convicted criminal at worst. I still don't know who owned that profile.

Another flaw of the voluntary code is that, while it covers sexual misconduct, serious mental and physical harm and child exploitation, it does not make provision for financial harm.

Given what we know about the extensive number of fake dating profiles being used to steal money from innocent victims (as well as the self reported statistics on the number of inauthentic accounts), this seems to be an oversight.



A report by TSB bank in the UK revealed 42 per cent of romance scam cases started on dating apps. In October, I requested the code be adjusted to include financial harm. The most recent response is that this will be considered as the first formal review approaches.

Also to be considered are broader regulatory developments including the Scams Prevention Framework – which does not cover dating platforms – and the Online Safety Act.

We have seen governments intervene previously when self-regulation has not worked. Australia is leading the world on age assurance and identity verification in social media for under-16s. The world is watching (and following) closely.

We must extend this thought leadership beyond the protection of children to adults on dating apps where robust and mandatory ID verification seems the only logical and safe next step.

Think about the last time you were required to prove who you are. When you opened a bank account. Applied for a mortgage. Registered a SIM card. When you bought pseudoephedrine at a pharmacy or signed a lease on an apartment. When you got a job, bought a car on finance, registered to vote, checked into a hotel or accessed a government service online.

Each one of those transactions – from the mundane to the consequential – requires you to prove, to a legally accountable standard, that you are who you say you are.

But to access an app that will put you in private, intimate, unsupervised contact with a complete stranger – potentially in their home, potentially alone, potentially after dark – you need nothing but an email address and a selfie.

The question is not whether we know how to verify identity at scale: we do it every day, for transactions far less dangerous than these. The question is why we have decided that the safety of women on dates is worth less than the sale of some cold and flu tablets at a chemist.

In addition to voluntary ID verification dating app solutions there are other more robust options out there. One is DKYC – (Dating Know Your Customer) – a purpose-built identity certification system for dating platforms. It is the world's first patent-pending technology of its kind, and it was built in Australia by Securely Group, based in Noosa, Queensland.

DKYC certifies dating profiles against regulated identity sources: bank KYC records, sovereign digital identity wallets, government-issued credentials. Not stored. Not exposed. Certified – meaning a platform receives a machine-readable confirmation that an account is bound to a verified, accountable identity, without ever accessing the underlying personal data.

Most importantly you can only use your real name, you cannot run or hide with this technology. It also includes biometric deduplication. When a new profile is certified, it is checked against a database of existing certified identities. One person. One certified identity.

A convicted fraudster running four profiles under four aliases across four platforms becomes – structurally – far harder to sustain. And when a ban is imposed, it sticks.

Persistent identity anchoring means re-entry under a new account fails at certification. Certification is also not a one-time check at signup. It operates as a continuous assurance process, re-evaluated at defined intervals and triggered by risk events.

An incarcerated person whose circumstances change would fail recertification. The profile goes dark. Not because a platform received a tip-off and processed a

Continued p40