Source: *The Straits Times,* pB2
Date: 29 May 2026

What PayNow's alias removal really signals

Combating scams is only part of the story. The move pushes Singapore towards a more auditable payments infrastructure.

Daniel Rabetti

For Singapore as a global financial hub, maintaining credibility in anti-money laundering enforcement is increasingly important, says the writer. International financial centres are now judged not only by efficiency and innovation, but also by their ability to monitor and control illicit financial activity. ST PHOTO: LIM YAOHUI

Singapore's decision to remove the alias or nickname option from PayNow has been presented as a move to combat impersonation scams. The logic is intuitive: If users see a name closer to the recipient's legal identity, deception becomes harder.

But the deeper significance of the change likely lies elsewhere.

The removal of aliases is not just about scams. It is part of a broader shift towards a more traceable and formalised digital payments infrastructure, one in which transactions are increasingly tied to verified real-world identities. In that sense, the move says as much about anti-money laundering, regulatory oversight and the monitoring of financial flows as it does about consumer protection.

That does not mean the scam rationale is false. Impersonation scams are a genuine and growing problem in Singapore. But there is a risk in presenting the policy primarily through that lens. It may create the impression that displaying partially verified names substantially improves safety, when most scams today rely less on identity ambiguity and more on behavioural manipulation, urgency and social engineering.

The more important question is therefore not only whether this change reduces scams, but also what kind of financial system it gradually creates in the process.

THE ILLUSION OF 'MORE INFORMATION, MORE SAFETY'

The move away from aliases rests on a reasonable intuition. Informal display names create ambiguity, and ambiguity can be exploited. A payment request from a familiar nickname may conceal a very different underlying identity.

Yet the replacement is not full transparency. Names will instead be partially masked, revealing fragments of a person's legal name without displaying it in full.

In practice, this may create a false sense of reassurance more than genuine verification. Singapore's naming conventions are structured enough that partially masked names can often still be inferred, especially when combined with a phone number or contextual information. A format such as "ChXX ShX HuX JacquXXXXX" may appear anonymised on paper, but in reality it is often not difficult to reconstruct the likely full name, particularly within Singapore's relatively structured naming environment.

At the same time, scammers rarely depend solely on identity ambiguity. Most successful scams exploit urgency, authority and trust, dynamics that a partially masked legal name does little to eliminate.

The risk is that users interpret a more formal-looking identity system as a stronger guarantee of safety than it actually provides.

A NEW ATTACK SURFACE: DATA HARVESTING

The privacy concerns are also not trivial. By linking phone numbers more closely to legal identities, the system potentially makes personal information easier to aggregate across platforms.

While large-scale automated querying would depend on the technical safeguards implemented by banks and payment providers, the broader concern is understandable. Even partially revealed identities can become valuable when combined with leaked data sets, social media profiles or other digital traces.

Hong Kong's experience offers a cautionary note. Its Faster Payment System (FPS) adopted a similar partial-masking approach, yet scam activity continued to rise in subsequent years. Police identified more than 22,000 FPS proxy accounts linked to scams in the first nine months of 2020 alone, while fraud losses through the platform exceeded HK$600 million (S$98 million) within months of new anti-scam measures being introduced.

At the same time, publicly available evidence does not clearly show that partial name disclosure materially reduces fraud relative to other regional systems that use different identity-display approaches. The Association of Banks in Singapore has cited Hong Kong's design as a reference point, but the comparative evidence remains limited.

THE BIGGER PICTURE: TRACEABILITY, TRANSPARENCY

The more important implication of the policy may therefore lie beyond scam prevention.

PayNow increasingly functions as part of Singapore's core financial infrastructure. Linking transactions more directly to verified identities strengthens the ability of banks and regulators to monitor financial flows, identify suspicious activity and comply with tightening anti-money laundering standards.

This matters in the current regulatory environment. The Monetary Authority of Singapore (MAS) has significantly intensified its anti-money laundering focus following several major financial scandals and increasing international scrutiny of illicit flows through global financial centres. In July 2025, MAS revised its anti-money laundering framework to align more closely with standards set by the Financial Action Task Force (FATF), the international body responsible for coordinating anti-money laundering rules.

PayNow increasingly functions as part of Singapore's core financial infrastructure. Linking transactions more directly to verified identities strengthens the ability of banks and regulators to monitor financial flows, identify suspicious activity and comply with tightening anti-money laundering standards.

Around the same period, MAS issued nearly $1 million in penalties to payment firms for anti-money laundering breaches under the Payment Services Act.

Viewed in that context, the removal of aliases looks less like a narrow anti-scam measure and more like part of a broader transition towards a fully auditable digital payments infrastructure.

A payment system built around verified identities is easier to integrate into compliance systems. Banks can more effectively flag suspicious transaction patterns, connect accounts across institutions and identify networks associated with fraud, sanctions evasion or illicit financing.

The implications extend beyond large criminal activity. As PayNow becomes deeply embedded in everyday commerce, from freelancers and tutors to hawkers and small online businesses, a more traceable payment infrastructure also gradually reduces the boundary between the formal and informal economy.

Whether or not taxation is an explicit objective, systems built around verified and traceable transactions naturally make income flows more visible over time. This can improve financial transparency and reduce illicit activity, but it also changes the relationship between citizens, small businesses and the financial system itself.

For Singapore, there are clear strategic reasons to move in this direction. As a global financial hub, maintaining credibility in anti-money laundering enforcement is increasingly important. International financial centres are now judged not only by efficiency and innovation, but also by their ability to monitor and control illicit financial activity.

The trade-off, however, should be stated clearly. A more traceable system may improve compliance and enforcement while also reducing privacy and anonymity in everyday financial interactions.

ALTERNATIVE DESIGNS AND SAFEGUARDS

The current approach is not the only option available. More sophisticated alternatives already exist. Many digital platforms signal authenticity without revealing full legal names, whether through verification markers, consistent account identifiers or contextual trust signals based on how well two parties know each other.

A large payment to an unfamiliar recipient warrants more scrutiny than a small transfer between friends. There is also a case for giving users some control over how they appear within clear boundaries. Allowing individuals to choose which parts of their name are displayed could preserve both recognisability and discretion for freelancers and small businesses that rely on PayNow for everyday transactions.

The strongest near-term safeguard, however, is likely technical rather than visual. Strict limits on automated lookups, detection of unusual querying patterns and clear rules governing how identity information can be accessed at scale are probably more important than the exact masking format shown on a screen.

Without such safeguards, the risk is that the system addresses the visible surface of the problem while leaving the underlying data infrastructure more exposed.

Fixing one problem should not mean obscuring another.

Ending PayNow aliases may reduce certain forms of impersonation scams. But its deeper significance lies elsewhere. The policy pushes Singapore's payment infrastructure towards a system where financial activity is increasingly linked to verified real-world identities.

That may ultimately prove beneficial for anti-money laundering enforcement, financial integrity and Singapore's position as a trusted global financial centre. But if that is the direction of travel, it deserves to be discussed openly and honestly.

Singapore has earned its reputation as a financial hub by calibrating efficiency, trust and regulation carefully. Trust in a payment system depends not only on knowing who you are transacting with, but also on understanding how your own financial information can be observed, connected and used.

The removal of PayNow aliases is therefore not just a design adjustment. It is part of a broader shift in how digital financial systems balance privacy, traceability and financial transparency. That broader conversation is one worth having explicitly.

• Daniel Rabetti is the S. Dhanabalan Chair in Quantitative Studies and a PYP assistant professor in accounting and finance at the National University of Singapore Business School. The opinions here are the writer's own and do not represent those of NUS.