

Scams, exclusion and the risks of digital finance

The price of progress demands a whole-of-society response. BY PIYUSH GUPTA

WHILE digitalisation has enabled great convenience and a better customer experience, it has also brought with it a new set of risks and challenges, and shifted the nature of risk in the financial sector.

Consumers worry about the risk of financial exclusion if they don't move to a digital platform, and the risk of scams and fraud if they do.

Financial institutions face heightened operational and liquidity risks. The need to balance financial stability, consumer trust, and innovation has been most evident in this area. And the regulators have had to play a very nuanced role.

Bridging the digital divide

Let's start with the issue of financial inclusion. Research has shown that the cost of a cash-based system amounts to almost 2 per cent of gross domestic product. In addition, paper forms of money, including cheques, give rise to delayed settlements and other related costs.

It therefore makes sense to move to digital payments for the country as a whole. However, it is also true that the digital shift gives rise to the risk of a digital divide.

This digital divide impacts less technology-savvy consumers, who typically include older, lower-income and less educated individuals. Industry regulators are trying to ensure balance and calibration in the face of change, including continuously adapting targets for cheque elimination.

Efforts have been made to uplift the digital capabilities of all consumers.

The Infocomm Media Development Authority (IMDA) has launched the Seniors Go Digital programme; banks have introduced programmes to boost financial literacy and promote digital inclusion.

I spent many a Saturday morning at hawkers' centres, sitting with elderly people, showing them how to use PayNow on their mobile phones. These initiatives have paid off, according to IMDA.

The percentage of seniors using online payments more than doubled from 38 per cent in 2018 to 78 per cent in 2022. Nonetheless, bridging the digital divide remains a constant work in progress and requires a close partnership among all participants.

Who is accountable for losses?

One of the biggest challenges of digitalisation is the growing scourge of scams. In 2024 alone, the number of scam cases increased by 11 per cent to about 51,000, with total losses rising by 70 per cent to over a billion dollars.

While scams have always existed, a digital world allows money to flow at a scale and speed that is very different from the physical world. The tension between trust, simplicity and innovation is most visible in this area.

Establishing accountability is difficult. While scammers are the clear villains, the parties accountable for the losses are often not so clear.

There are generally two types of scams: Authorised scams are when victims are tricked by fraudsters into transferring money by themselves. But in unauthorised scams, the fraudster transfers the funds without authorisation from the individual.

Last year, four of the top five scam types in Singapore were authorised scams. Some of these include impersonating individuals such as friends while others involve tricking individuals into transferring money to gain something in return, such as job scams, investment scams and love scams.

In such "authorised" scams, it seems obvious that the individual should be accountable for the loss. However, the question is often raised about whether financial intermediaries



While scams have always existed, a digital world allows money to flow at a scale and speed that is very different from the physical world.
PHOTO: BT FILE

could step up to help their customers protect themselves.

In unauthorised scams, such as phishing scams, since the victim did not intend to make payment, should the buck stop at the bank? Even here, banks argue that the victim is at least partly complicit.

Some argue that other players in the system could do more. For example, should telcos be held accountable for these scammers who send SMSes with malicious links? Or should social media and e-commerce players exercise more care in establishing the bona fides of their users?

Establishing accountability is not easy. Determining how to share the financial burden is very tricky.

If losses are fully borne by institutions, then individuals may lose the incentive to remain vigilant. If individuals bear full responsibility, then financial institutions may lower their standards for safeguarding the consumer. This is what is best known as a moral hazard.

Systemic change needed

Given that the shift to a digital economy is so redefining, some people argue, like me, that a whole-of-society shift is required.

One can draw the analogy from the transition of the stagecoach to the motor car.

The responsibility of shifting towards a car-based society fell not only to the car companies, but also to the authorities who implemented infrastructures such as pavements, zebra crossings, traffic lights, as well as pedestrians who had to learn to look left and look right before crossing roads, and drivers who had to learn how to observe traffic rules.

This was a whole-of-society reform. Likewise, dealing with scams and fraud requires a similar structural shift in the entire ecosystem, involving players such as regulators, financial institutions, telecom companies, social media companies, government agencies, law enforcement agencies and individuals.

Reconfiguring the current framework, processes and mindset is not a matter of choice, but one of necessity.

Recognising the need to implement collective defences, the financial industry, the police and other government agencies have collaborated to implement holistic measures, including a Shared Responsibility Framework implemented by the Monetary Authority of Singapore and IMDA in 2024.

This framework assigns respective duties to individuals, financial institutions and telecom companies, setting out the accountability of national institutions and providers for losses incurred.

For instance, it requires financial institutions to implement measures such as real-time fraud surveillance and block transactions that

result in significant draining of accounts.

The industry has also come together to work proactively with regulators. The Association of Banks in Singapore's (MAS) Standing Committee on Fraud aligns with the banking sector on all of the Republic's initiatives to address these scams.

More recently, banks enhanced safeguards for digital transactions by deliberately adding friction, such that if large transactions resulting in more than 50 per cent of an account's balance is being transferred at one time, there will be a pause. The transaction would be put on hold for 24 hours or rejected on credit.

Such actions seem counter-intuitive, but they are a good example of the trade-offs that need to be made to retain customer trust.

Similarly, in another counter-intuitive move, the Protection from Scams Bill was passed, allowing the police to order banks to temporarily restrict the banking transactions of potential scam victims.

An important balancing act

The scam issue highlights key tensions between competing goals, including that between innovation and trust, as well as enabling trust while preventing moral hazard.

The tension between innovation and trust also plays out in the sphere of artificial intelligence (AI) and data. I have written about the risk of discrimination and red-lining. And the question of balancing efficiency against social goals of helping the disadvantaged remains.

The insurance industry offers another example. It is built on the fundamental premise that no one knows where the risk is, so we socialise the risk. But once we start to know who will fall sick and who will not, those who know they are not going to get sick will not pay the premium. And no one will insure those who are certain to get sick.

In view of the potential misuses of AI and data, MAS and the industry have collaborated to put in place the necessary governance and ethical frameworks. The ever-evolving nature of these risks means that the arguments and measures against them will be a constant work in progress.

As in the past, the public, private and people sectors must continue to work together, in close collaboration, to get the balance right – staying on the edge of innovation while protecting trust and stability at the same time.

The writer is the 17th S R Nathan Fellow at the Institute of Policy Studies (IPS). He was the former chief executive officer and director of DBS Group.

This is an edited excerpt of the second IPS-Nathan Lecture by the writer on Singapore's financial sector.