**Publication: The Straits Times, pg B1, B2**
**Date: 12 January 2023**
**Headline: Should e-commerce platforms bear the losses from scams?**

# *Should e-commerce platforms bear the losses from scams?*

Contract law is premised on the principle of buyer beware, but the dynamics of digital marketplaces demand a new approach

**Mark Findlay**

The biggest myth about e-commerce platforms is that they do nothing more than bring sellers and buyers together. If this were so, then Carousell and the like would be charitable services doing the public a service by filling a need yet charging nothing.

But reality suggests otherwise. In fact, online marketplaces can be dangerous spaces where trading goods and services can feel like sketchy exchanges in the absence of laws or other strong regulations ensuring the security, safety and authenticity of such transactions and proportioning losses arising from fraud.

That problem has grown in Singapore since the pandemic following the explosion of e-commerce, particularly in consumer marketplaces. At least 877 people have been duped by fake buyers on Carousell in December 2022 alone, with losses totalling $836,000.

Scammers posing as buyers would ask sellers for contact details so that they can send out fake links to complete purchases. Many users were duped into giving up their banking details including one-time passwords and login credentials, only to realise they had been scammed after unauthorised transactions were made.

The losses can rack up quite a bill. From cheap tickets to Universal Studios Singapore to discounted hotel room bookings and vaccinated travel lane seats that never materialised, over $8.3 million alone was lost in such e-commerce scams in the first half of 2022. Police reports of such cases doubled in that same period compared with 2021.

Why do the victims of such scams bear the losses today? A fundamental principle of contract law is *caveat emptor* or "buyer beware", which puts the onus on the purchaser to exercise due diligence to secure a successful transaction that meets his or her expectations.

But that principle was cast in days when buyers could physically inspect goods and services before handing over money. In today's digital world, scams involving buyers parting with crucial personal financial information suggest a lack of caution needed on both the buyers' part and the platforms enabling the transaction.

There is also little a single individual can do to unmask subtle fraud, in a world where we are constantly bombarded by fraudsters on our smartphones with fake messages from the supposed Ministry of Health and more. Scam filters like ScamShield can help detect scam SMSes but end up engendering lazy behaviour instead of encouraging vigilance.

## WHOSE RESPONSIBILITY?

Should Singapore then move the pendulum of responsibility for scam losses towards platforms, similar to the approach taken by Britain's Online Safety Bill?

The Bill requires online platforms to protect users against both user-generated scams and fraudulent advertisements via "proportionate systems and processes"; to "minimise the length of time such fraudulent advertising is present on the service; and to swiftly take down such content once alerted to its presence". The emphasis of this approach is prevention of loss through direct action against fraudulent material.

Other countries, like Singapore, prefer deterrence and collaboration – with stiff penalties for scammers to deter crime along with industry collaboration to improve user awareness of such perils.

Home Affairs and Law Minister K. Shanmugam had highlighted this strong deterrence against scammers, with imprisonment of up to 10 years when the issue of stiffer laws against e-commerce scams was raised in Parliament in 2022.

But he also noted the challenge of tracking and recovering lost money when transactions are routed overseas, given the need for telcos, banks and law enforcement agencies in other jurisdictions to work together. In one infamous case of undelivered luxury goods worth $32 million, collaboration with the Royal Thai Police provided intelligence on the location of the culprits while working with the Malaysian authorities was crucial in nabbing the couple in Johor, where they had absconded to.

If anything, such cases illustrate how crooks are less deterred by fines or prison time when the prize money is huge and the chances of getting caught are slim.

CONTINUED ON PAGE B2

**Publication: The Straits Times, pg B1, B2**
**Date: 12 January 2023**
**Headline: Should e-commerce platforms bear the losses from scams?**

# *Rebalance of risk worth exploring*

FROM B1

Improving access to information has been key to the second strategy of improving public education, particularly at the last mile. An Inter-Ministry Committee on Scams launched an E-commerce Marketplace Transactions Safety Ratings (TSR) in May 2022, which assigns an overall safety rating based on the measures in place to ensure user authenticity, transaction safety and the availability of remedial channels.

Such safety ratings can be an important initiative and best practice that gives online users a risk assessment shorthand to fall back on. Amazon, Lazada and Qoo10 have been awarded four ticks, whereas Shoppe has three, Carousell two and Facebook Marketplace just one.

But this honours-based TSR relies on self-reporting by platform firms. How ratings are set up, monitored and audited is not explicit. For example, it is uncertain how platforms verify user identities, what actions they must take to be deemed to have fulfilled the criteria for monitoring fraudulent seller behaviour, and what thresholds are set regarding the maintenance of transaction records and user data.

Consequently, to what extent each measure has been effective in tackling scams and what further enforcement measures are needed are unclear. Such an approach is also premised on and aimed at strengthening the buyer beware principle in tackling scams, where the onus still falls on users to exercise reasonable caution. There is a limit to what the buyer can do without relying on the best practices of the platforms.

In essence, this strategy is silent on the degree of responsibility for losses arising from scams that should be borne by the platforms – the firms making money out of our transactions and transaction data.


## THE CASE FOR ONLINE MARKETPLACES

Singapore has much riding on propagating rules of the road in the digital realm, considering its strong stated desire to accelerate its national digital transformation and expand digital trade. With Digital Economy Agreements inked with Chile, New Zealand, Australia, United Kingdom and South Korea, Singapore aims to foster common standards and systems that support businesses engaging in digital trade and e-commerce, including regulations guarding against fraudulent, misleading or deceptive exchanges.

The reputation of digital commerce and the confidence of consumers here are important factors in whether Singapore is seen as a model worth emulating, and impacts whether the country can successfully expand its digital trade footprint elsewhere.

In these exchanges, while buyers, sellers and users have a role to play in responsible e-commerce trading, platforms stand to gain exponentially, from expansion into new markets and multiplying effects with insights from transaction data. South-east Asia's digital economy alone may be worth US$1 trillion (S$1.3 trillion) by 2030, a report by Temasek, Google and Bain in October 2022 reveals.

## TRUST, THE CURRENCY E-COMMERCE PLATFORMS NEED

This is not to say that digital marketplaces are the Wild Wild West. Far from it. E-commerce sites thrive on trust. They know fraud undermines their credibility. If buyers and sellers are not confident their information will be carefully managed and transactions can be conducted safely, they may exit the platform and choose from a plethora of other competitors.

For this reason, many have some form of recourse for buyers and sellers who find themselves in tricky situations. Some like Amazon offer money-back guarantees on certain deals. E-Bay offers mediation services even when not required by law to do so.

Many platforms know their reputation and the future of their business can hang on the question of whether they offer sufficient protections for users.

Carousell agrees it has a "duty of care" but has focused on education, safety advisories, authenticating "verified" users and encouraging the use of secure payment solutions provided by the platform. What criteria it employs for verification remains a matter for the platform, and as such is not open to customer scrutiny.

**E-commerce platforms that hide behind the responsibility of buyers and the law risk their reputations and the stability of the market. As the subprime mortgage market crash in the US in 2008 worryingly revealed, confidence in the financial system can vanish overnight when powerful market players able to externalise damage onto others are subject to lax rules.**

In cases of phishing, the most common type of scam on Carousell, a warning pops up urging users to examine any links before making a transaction. Such actions help to alert the user at point of purchase to scams but responsibility remains squarely with the user.

Yet the fact that scams are not only persisting but growing begs the question of whether more can be done. The answer must be a resounding yes.

## GREATER 'SMART' REGULATION NEEDED

Regulating e-commerce platforms will be a tall order but is not an impossible task. The authorities should bear in mind a few key trade-offs.

First, regulation will have to balance security and user experience. Overly aggressive and intrusive validation barriers may kill the convenience of platform marketing which is a big factor in the explosion of digital marketplaces. Know-your-customer measures such as facial recognition and document verification employed to keep fraudulent actors away from the system can also raise significant issues around privacy and personal data protection.

But requiring people to go through some hassle to guarantee the security of transactions and requiring platforms to do due diligence in authenticating users seems like a worthwhile exchange. As a baseline, platforms should be mandated to carry out due diligence on risky offers and take down non-compliant posts. These online marketplaces have big data on scamming patterns and the power to intervene before users are tricked into handing over cash or banking details.

Another option worth exploring is a compensation model taking the form of a no-fault insurance, but this would not be popular with the platforms. However, taking note of Volkswagen's position on paying damages for autonomous vehicle accidents, the reputation of the marketplace should outweigh any business cost increases. Compliance costs should not have priority over the societal benefits of greater confidence in e-commerce.

E-commerce platforms that hide behind the responsibility of buyers and the law risk their reputations and the stability of the market. As the subprime mortgage market crash in the US in 2008 worryingly revealed, confidence in the financial system can vanish overnight when powerful market players able to externalise damage onto others are subject to lax rules.

What is at stake here also goes beyond the dollars and cents lost by careless buyers and extends into the realm of market confidence in fledgling e-commerce at a time when sales volumes post-pandemic may be tapering off, as well as when the long-term success of digital transformation is at stake.

So should e-commerce platforms bear losses from scams? The answer is yes but the details are worth looking into. If the shift into digital makes individuals take on more risk including the responsibility of loss when the big players are profiting, then a rebalance is surely worth exploring.

• Professor Mark Findlay is a faculty member of the Yong Pung How School of Law at the Singapore Management University, and professorial fellow at the Centre for AI and Data Governance at SMU.