COMBATTING SCAMS IN AUSTRALIA, SINGAPORE, CHINA AND HONG KONG

Date: 17 April 2025

Australia Finance Alert

By: Claudine Salameh, Tamsyn Sharpe

Key Points:

- *Singapore's Shared Responsibility Framework*
- *Comparing scams regulation in Australia, Singapore and the UK*
- *China's Anti-Telecom and Online Fraud Law*
- *Hong Kong's Anti-Scam Consumer Protection Charter and Suspicious Account Alert Regime*

The increased reliance on digital communication and online banking has created greater potential for digitally-enabled scams. If not appropriately addressed, scam losses may undermine confidence in digital systems, resulting in costs and inefficiencies across industries. In response to increasingly sophisticated scam activities, countries around the world have sought to develop and implement regulatory interventions to mitigate growing financial losses from digital fraud. So far in our scam series, we have explored the regulatory responses in Australia and the UK. In this publication, we take a look at the regulatory environments in Singapore, China and Hong Kong, and consider how they might inform Australia's industry-specific codes.

SINGAPORE

Shared Responsibility Framework

In December 2024, Singapore's Shared Responsibility Framework (SRF) came into force. The SRF, which is overseen by the Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA), seeks to preserve confidence in digital payments and banking systems by strengthening accountability of the banking and telecommunications sectors while emphasising individuals' responsibility for vigilance against scams.

Types of Scams Covered

Unlike reforms in the UK and Australia, the SRF explicitly excludes scams involving authorised payments by the victim to the scammer. Rather, the SRF seeks to address phishing scams with a digital nexus. To fall within the scope of the SRF, the transaction must satisfy the following elements:

1. The scam must be perpetrated through the impersonation of a legitimate business or government entity;
2. The scammer (or impersonator) must use a digital messaging platform to obtain the account user's credentials;

©2005-2026 K&L Gates LLP. All Rights Reserved.

3. The account user must enter their credentials on a fabricated digital platform; and
4. The fraudulently obtained credentials must be used to perform transactions that the account user did not authorise.

Duties of Financial Institutions

The SRF imposes a range of obligations on financial institutions (FIs) in order to minimise customers' exposure to scam losses in the event their account information is compromised. These obligations are detailed in table 1 below.

Table 1

Obligation	**Description**
12-hour cooling off period	Where an activity is deemed "high-risk", FIs must impose a 12-hour cooling off period upon activation of a digital security token. During this period, no high-risk activities can be performed In activity is deemed to be "high-risk" if it might enable a scammer to quickly transfer a large sum of money to a third party without triggering a customer alert. Examples include: ▪ Addition of new payee to the customer's account; ▪ Increasing transaction limits; ▪ Disabling transaction notification alerts; and ▪ Changing contact information.
Notifications for activation of digital security tokens	FIs must provide real-time notifications when a digital security token is activated or a high-risk activity occurs. When paired with the cooling off period, this obligation increases the likelihood that unauthorised account access is brought to the attention of the customer before funds can be stolen.
Outgoing transaction alerts	FIs must provide real-time alerts when outgoing transactions are made.
24/7 reporting channels with self-service kill switch	FIs must have in place 24/7 reporting channels which allow for the prompt reporting of unauthorised account access or use. This capability must include a self-service kill-switch enabling customers to block further mobile or online access to their account, thereby preventing further unauthorised transactions.

©2005-2026 K&L Gates LLP. All Rights Reserved.

Duties of Telecommunications Providers

In addition to the obligations imposed on FIs, the SRF creates three duties for telecommunications service providers (TSPs). These duties are set out in table 2 below.

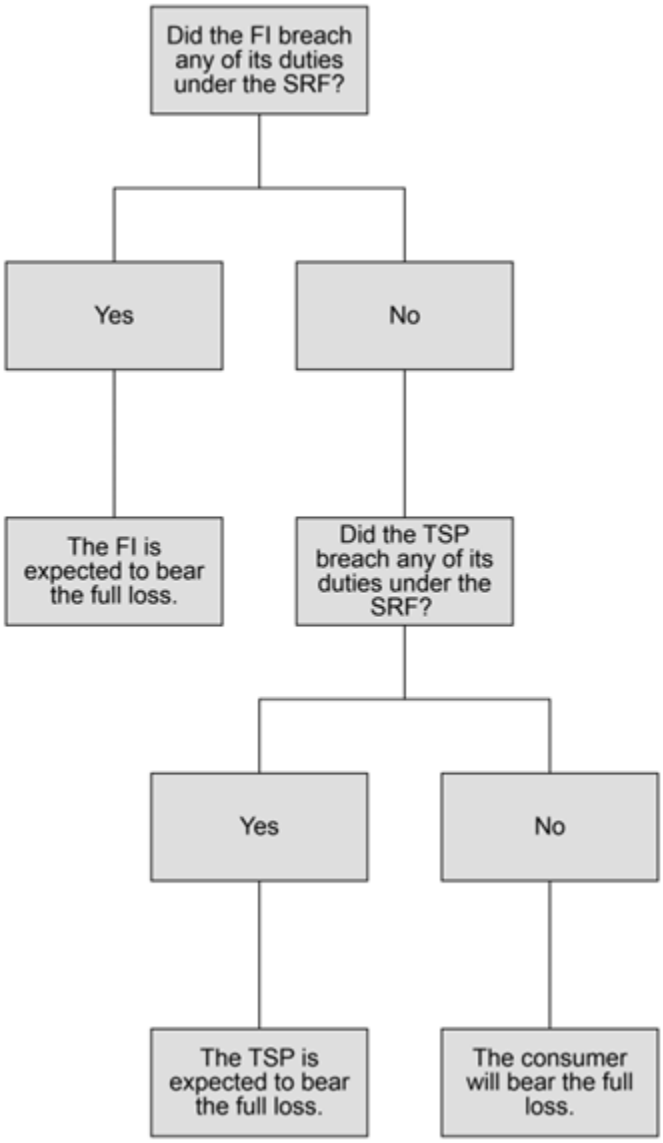
Table 2

Obligation	**Description**
Connect only with authorised alphanumeric senders	In order to safeguard customers against scams, any organisation wishing to send short message service (SMS) messages using an alphanumeric sender ID (ASID) must be registered and licensed. TSPs must block the sending of SMS messages using ASIDs if the sending organisation is not appropriately registered and licensed.
Block any message sent using an unauthorised ASID	Where the ASID is not registered, the TSP must prevent the message from reaching the intended recipient by blocking the sender.
Implement anti-scam filters	TSPs must implement anti-scam filters which scan each SMS for malicious elements. Where a malicious link is detected, the system must block the SMS to prevent it from reaching the intended recipient.

Responsibility Waterfall

Similar to the UK's Reimbursement Rules explored in our second article, the SRF provides for the sharing of liability for scam losses. However, unlike the UK model, the SRF will only require an entity to reimburse the victim where there has been a breach of the SRF. The following flowchart outlines how the victim's loss will be assigned.

©2005-2026 K&L Gates LLP. All Rights Reserved.



Source: Tamsyn Sharpe.

HOW DOES THE SRF COMPARE TO THE MODELS IN AUSTRALIA AND THE UK?

Scam Coverage

The type of scams covered by Singapore's SRF differ significantly to those covered by the Australian and UK models. In Australia and the UK, scams regulation targets situations in which customers have been deceived into authorising the transfer of money out of their account. In contrast, Singapore's SRF expressly excludes any scam involving the authorised transfer of money. The SRF instead targets phishing scams where the perpetrator obtains personal details in order to gain unauthorised access to the victim's funds.

©2005-2026 K&L Gates LLP. All Rights Reserved.

Entities Captured

Australia's Scams Prevention Framework (SPF) covers the widest range of sectors, imposing obligations on entities operating within the banking and telecommunications sectors as well as any digital platform service providers which offer social media, paid search engine advertising or direct messaging services. The explanatory materials note an intention to extend the application of the SPF to new sectors as the scams environment continues to evolve.

In contrast, the UK's Reimbursement Rules only apply to payment service providers using the faster payments system with the added requirement that the victim or perpetrator's account be held in the UK. Any account provided by a credit union, municipal bank or national savings bank will be outside the scope of the Reimbursement Rules.

Falling in-between these two models is Singapore's SRF which applies to FIs and TSPs.

Liability for Losses

Once again, the extent to which financial institutions are held liable for failing to protect customers against scam losses in Singapore lies somewhere between the Australian and UK approaches. Similar to Singapore's responsibility waterfall, a financial institution in Australia will be held accountable only if the institution has breached its obligations under the SPF. However, unlike the requirement to reimburse victims for losses in Singapore, Australia's financial institutions will be held accountable through the imposition of administrative penalties. In contrast, the UK's Reimbursement Rules provide for automatic financial liability for 100% of the customer's scam losses, up to the maximum reimbursable amount, to be divided equally where two financial institutions are involved.

CHINA

Anti-Telecom and Online Fraud Law of the People's Republic of China

China's law on countering Telecommunications Network Fraud (TNF) requires TSPs, Banking FIs and internet service providers (ISPs) to establish internal mechanisms to prevent and control fraud risks. Entities failing to comply with their legal obligations may be fined the equivalent of up to approximately AU$1.05 million. In serious cases, business licences or operational permits may be suspended until an entity can demonstrate it has taken corrective action to ensure future compliance.

Scope

China's anti-scam regulation defines TNF as the use of telecommunication network technology to take public or private property by fraud through remote and contactless methods. Accordingly, it extends to instances in which funds are transferred without the owner's authorisation. To fall within the scope of China's law, the fraud must be carried out in mainland China or externally by a citizen of mainland China, or target individuals in mainland China.

Obligations of Banking FIs

Banking FIs are required to implement risk management measures to prevent accounts being used for TNF. Appropriate policies and procedures may include:

©2005-2026 K&L Gates LLP. All Rights Reserved.

- Conducting due diligence on all new clients;
- Identifying all beneficial owners of funds:
- Requiring frequent verification of identity for high-risk accounts:
- Delaying payment clearance for abnormal or suspicious transactions: and
- Limiting or suspending operation of flagged accounts.

The People's Bank of China and the State Council body are responsible for the oversight and management of Banking FIs. The anti-scams law provides for the creation of inter-institutional mechanisms for the sharing of risk information. All Banking FIs are required to provide information on new account openings as well as any indicators of risk identified when conducting initial client due diligence.

Obligations of TSPs and ISPs

TSPs and ISPs are similarly required to implement internal policies and procedures for risk prevention and control in order to prevent TNF. This includes an obligation to implement a true identity registration system for all telephone/internet users. Where a subscriber identity module (SIM) card or internet protocol (IP) address has been linked to fraud, TSPs/ISPs must take action to verify the identity of the owner of the SIM/IP address.

HONG KONG

Hong Kong lacks legislation which specifically deals with scams. However, a range of non-legal strategies have been adopted by the Hong Kong Monetary Authority (HKMA) in order to address the increasing threat of digital fraud.

Anti-Scam Consumer Protection Charter

The Anti-Scam Consumer Protection Charter (Charter) was developed in collaboration with the Hong Kong Association of Banks. The Charter aims to guard customers against digital fraud such as credit card scams by committing to take protective actions. All 23 of Hong Kong's card issuing banks are participating institutions.

Under the Charter, participating institutions agree to:

- Refrain from sending electronic messages containing embedded hyperlinks. This allows customers to easily identify that any such message is a scam.
- Raise public awareness of common digital fraud.
- Provide customers with appropriate channels to allow them to make enquiries for the purpose of verifying the authenticity of communications and training frontline staff to provide such support.

More recently, the Anti-Scam Consumer Protection Charter 2.0 was created to extend the commitments to businesses operating in a wider range of industries including:

- Retail banking;
- Insurance (including insurance broking);
- Trustees approved under the Mandatory Provident Fund Scheme; and

©2005-2026 K&L Gates LLP. All Rights Reserved.

- Corporations licensed under the Securities and Futures Ordinance.

Suspicious Account Alerts

In cooperation with Hong Kong's Police Force and the Association of Banks, the HKMA rolled out suspicious account alerts. Under this mechanism, customers have access to Scameter which is a downloadable scam and pitfall search engine. After downloading the Scameter application to their device, customers will receive real-time alerts of the fraud risk of:

- Bank accounts prior to making an electronic funds transfer;
- Phone numbers based on incoming calls; and
- Websites upon launch of the site by the customer.

In addition to receiving real-time alerts, users can also manually search accounts, numbers or websites in order to determine the associated fraud risk.

Scameter is similar to Australia's Scamwatch, which provides educational resources to assist individuals in protecting themselves against scams. Users can access information about different types of scams and how to avoid falling victim to these. Scamwatch also issues alerts about known scams and provides a platform for users to report scams they have come across.

KEY TAKEAWAYS

Domestic responses to the threat of scams appear to differ significantly. Legal approaches explored so far in this series target financial and telecommunications sectors, seeking to influence entities in these industries to adopt proactive measures to prevent, detect and respond to scams. While the UK aims to achieve this by placing the financial burden of scam losses on banks, China and Australia adopt a different approach by imposing penalties on entities failing to comply with their legal obligations. Singapore has opted for a blended approach whereby entities which have failed to comply with the legal obligations under the SRF will be required to reimburse customers who have fallen victim to a scam. However, where the entities involved have met their legal duties, the customer will continue to bear the loss.

Look out for our next article in our scams series.

The authors would like to thank graduate Tamsyn Sharpe for her contribution to this legal insight.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



CLAUDINE SALAMEH
PARTNER

SYDNEY
+61.2.9513.2541
CLAUDINE.SALAMEH@KLGATES.COM



AYMAN GUIRGUIS
PARTNER

SYDNEY
+61.2.9513.2308
AYMAN.GUIRGUIS@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.