Fraud Resolution: Building Trust through Shared Accountability

Globally, consumers lost about USD442 billion to scams[1] in 2024. In Malaysia, the reported impact amounted to RM2.8 billion in 2025.[2] In these statistics, there are stories of real people suffering misfortune – a retiree who lost his entire life savings or a family whose emergency funds disappeared overnight.

This raises an important question: *When fraud happens, who should take responsibility and bear the losses? Is it the financial institution, the consumer, or should responsibility be shared more broadly across the digital ecosystem?*

This question touches on the aspect of trust within the financial system. Amid increasingly sophisticated fraud tactics, we need to ensure that digital payments remain safe and accessible, and that public confidence is upheld. Financial institutions must continue investing in technology to shore up their defences against fraud. At the same time, consumers need to be equipped with better tools and awareness to keep digital banking secure. But when fraud does happen, fairness must be upheld for both the consumer and financial institution. This should be supported by a robust investigation process to help justify a reasonable outcome for all parties. Ultimately, preventing fraud is a shared accountability. This accountability should also be reviewed over time as the role of other key digital players beyond the financial ecosystem become more prominent, reflective of the broader digital ecosystem.

Regulators worldwide recognise that ensuring fraud victims are treated fairly is just as important as strong prevention. Many countries are exploring compensation frameworks for victims alongside tighter security controls. However, developing this framework is not an easy task. It requires striking a balance between fairness, legal limits and ease of implementation. Even so, only a few countries have taken the step of introducing compensation frameworks. These frameworks are tailored to fit their respective fraud landscapes and regulatory environments (Table 1).

For Malaysia, BNM introduced a compensation framework in 2024 through the Policy Document on Ensuring Fair Treatment for Victims of Unauthorised e-Banking Transactions (SEFT). The policy currently focuses on unauthorised transactions.[3] SEFT promotes a shared approach to accountability between banks and their customers (Diagram 1). This is done without compromising the need for ongoing customer vigilance. While SEFT provides a basis for considering compensation, it does not guarantee compensation to victims in all cases. The policy recognises that, in some cases, liability should be shared and not rest with just one party.

SEFT provides a clear and transparent framework for assessing cases, ensuring customers are aware of their rights. The framework also clarifies the respective roles of both the banks and customers in preventing fraud. For instance, customers are expected to avoid risky actions, such as clicking on unknown links which could lead to the unintentional sharing of their passwords. At the same time, banks remain accountable for failing to detect and prevent suspicious transactions that occur outside customers' normal behaviour. There are also cases where the victim is held fully responsible for the fraud and therefore should not be eligible to any compensation. For example, when a victim refuses to cooperate with the bank during the investigation or proceeds to download harmful mobile applications despite prior warnings from the bank of its risks. Through this approach, SEFT reinforces the principle of shared accountability. It emphasises that both banks and customers play an active role in safeguarding the integrity of digital payments.

---

1 Global State of Scams 2025 Report by Global Anti-Scam Alliance (GASA).

2 As per data by Polis Diraja Malaysia (PDRM) that includes telecommunication scam, e-commerce scam, loan scam, investment scam, love scam as well as malware and phishing.

3 These refer to transactions made by fraudsters without the victim's knowledge. Fraudsters use methods like malware and phishing to obtain personal credentials of their victims. Once compromised, fraudsters use these credentials to perform unauthorised transactions. This excludes cases where customers initiate transactions themselves, including those made under coercion or undue influence, such as love or investment scams.

Table 1: Comparable Frameworks At a Glance

	Malaysia[1]	United Kingdom[2]	Singapore[3]	Thailand[4]
Scope	Unauthorised transactions	Authorised push-payment fraud (APP)	Phishing-linked unauthorised transactions	Authorised and unauthorised payment fraud
Effective date	October 2024	October 2024	December 2024	April 2025
Parties involved	1. Banks 2. Customers	1. Banks and payment service providers 2. Customers	1. Banks and payment service providers 2. Telecommunication providers (Telcos) 3. Customers	1. Banks and payment service providers 2. Digital asset operators 3. Telcos 4. Social media platform providers 5. Customers
Core principle	Clear and timely case management process; shared accountability between banks and customers, accounting for their respective obligations	Mandatory reimbursement, with sending and receiving institutions equally sharing the loss, unless customer was found to be acting with gross negligence	Shared responsibility with loss to be fully borne by a party that fails to meet its obligations, based on a clearly defined hierarchy: bank or payment service provider ⟶ telco ⟶ customer	Shared responsibility with parties breaching duties paying the loss

[1] The policy document can be found here: (*https://www.bnm.gov.my/documents/20124/938039/Ensuring_Fair_Treatment_for_Victims_of_Unauthorised_eBanking-Transactions.pdf).*

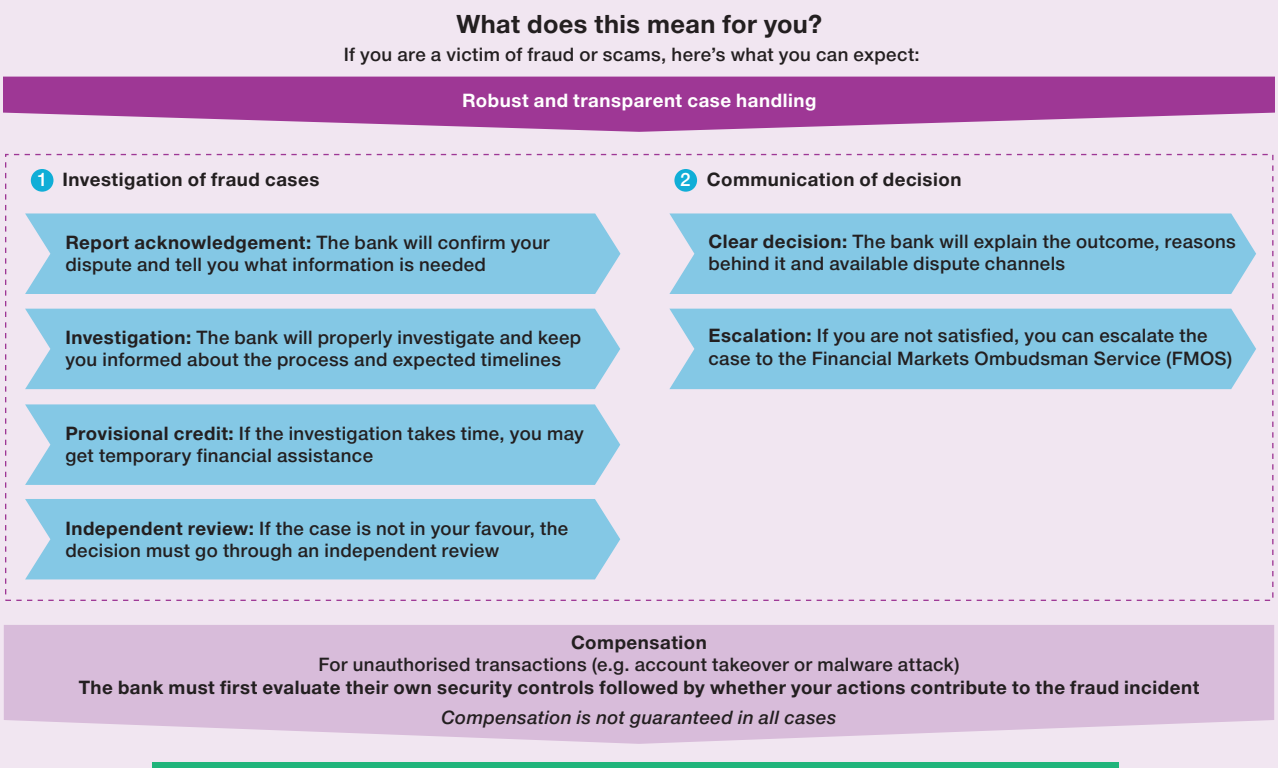
[2] UK's APP scams reimbursement requirement (*https://www.psr.org.uk/publications/policy-statements/ps255-app-scams-reimbursement-requirement/*).

[3] Singapore's Guidelines on Shared Responsibility Framework (*https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework*).

[4] Thailand's Emergency Decree on Measures for the Prevention and Suppression of Technological Crime (No. 2) (2025) (*https://www.bot.or.th/th/news-and-media/news/news-20250428.html*).

Source: Bank Negara Malaysia

Diagram 1: Understanding the Key Principles of SEFT



Source: Bank Negara Malaysia

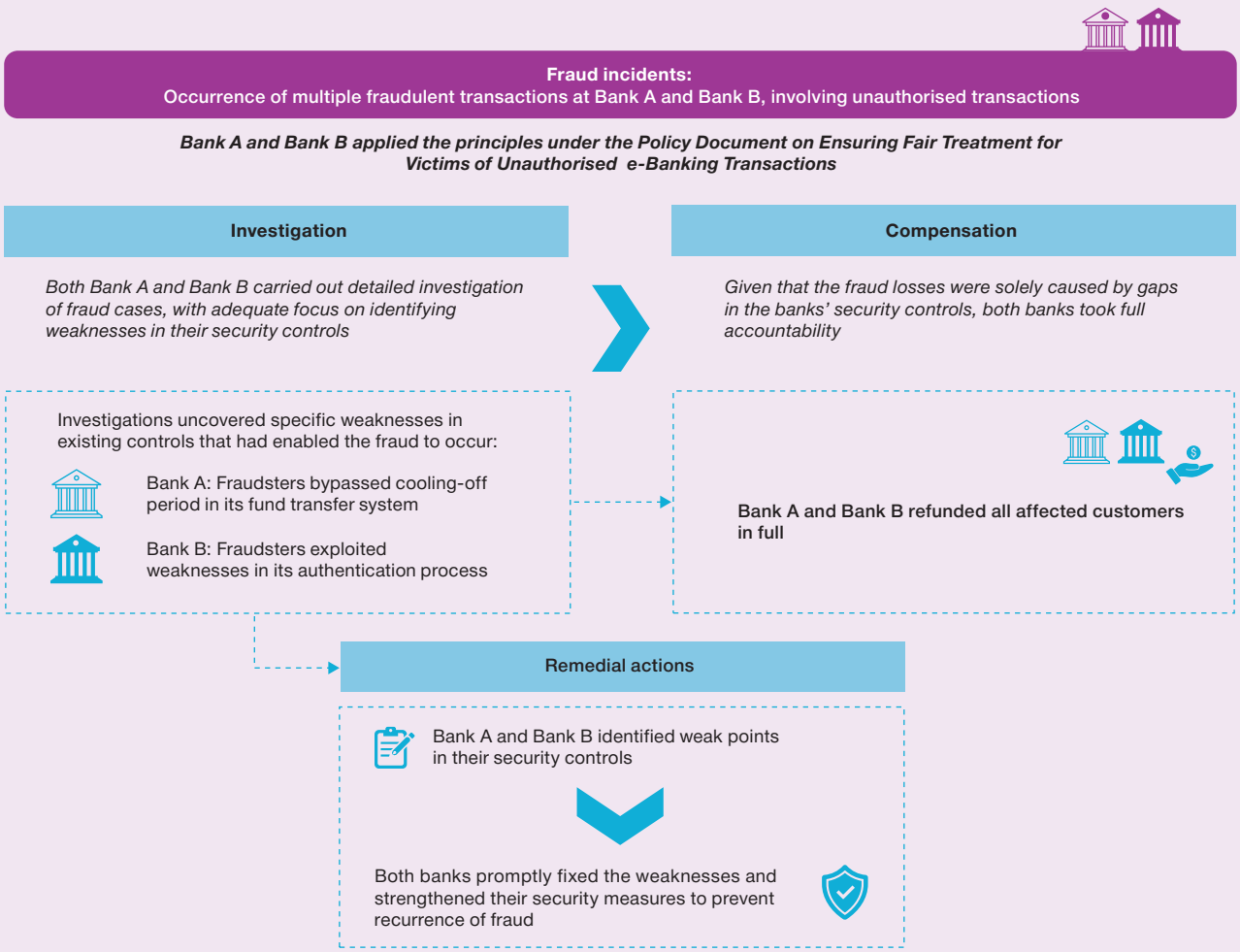
From Policy to Practice: One Year On

SEFT came into effect in October 2024. Since then, BNM has been closely monitoring banks' implementation. The initial focus has been on how banks manage fraud cases and allocate fraud losses. *So, has SEFT really made a difference?*

We have begun to see encouraging signs (Diagram 2). Initial findings show that SEFT has made banks more accountable and transparent in carrying out investigations. This is validated by an increase in the number of victims receiving either full or partial compensation in 2025 by about 26% compared to the previous year. Banks have also taken proactive steps to strengthen malware defences, with some reporting zero malware cases in 2025. This pre-emptively prevents unauthorised transactions, thereby reducing the need for reactive compensation. Some improvements attributed to SEFT implementation include:

- ***Greater accountability in investigation:*** Banks check for weaknesses in their systems first before placing any accountability on customers. In several cases, banks fully absorbed losses upon identifying system weakness.
- ***Greater transparency around customer rights:*** Banks inform victims upfront of their rights during the investigation process. Banks are showing greater consistency in completing investigations within the expected 14-day timeline. This reflects timelier case management, while maintaining the rigour of the process. For cases that take longer, banks are offering temporary financial assistance to help victims with daily needs.
- ***Faster system fixes:*** Compensation decisions push banks to address system weaknesses more quickly.

Diagram 2: An Illustration of the Impact of SEFT



Source: Bank Negara Malaysia

These developments not only safeguarded consumers' interests but also paved the way for quicker fixing of control gaps. In turn, these led to further strengthening of security and trust in the overall banking system.

Where We Need to Raise the Bar

While progress is clear, further areas for improvement include:

- ***Navigating shared accountability amid evolving fraud risks:*** Fraud cases are becoming more complex as tactics continue to evolve. It is much harder to distinguish between genuine and fraudulent interactions and attribute culpability. This adds to the challenges in implementing a fair compensation framework.

  Recognising this, SEFT offers a structured approach to assigning accountability, fostering clarity and consistency in how cases are assessed. Under SEFT, banks must first assess the effectiveness of their own controls before considering customer actions. This ensures case reviews are balanced and support the reasoning behind case outcomes, even in complex situations. As implementation of SEFT matures, BNM expects increased consistency in how shared accountability is implemented. Such consistency will be key in maintaining trust in resolution outcomes.

- ***Access to alternative dispute resolution channels:*** Compensation offered by a bank is not the end of the process. Many customers remain unaware of their rights and channels available if they are not happy with compensation offered by the bank.

  Customers can dispute the bank's decision by bringing their case to the Financial Markets Ombudsman Service (FMOS).[4] Banks must make this channel known to customers and remind them of its availability. This ensures that consumers can exercise their rights with confidence.

Looking Ahead

The first year of SEFT shows early alignment with the principles of fair treatment and shared accountability. However, the fight against fraud is far from over. In fact, it is an ongoing process. Further efforts to strengthen prevention, enforcement and recovery, as well as consumer protection continue to be pursued.

As knowledge is the most effective shield against scams and helps build a more vigilant society, efforts on consumer education are also being accelerated. This is especially important as about 95% of online fraud cases in Malaysia are authorised transactions.[5] Diagram 3 outlines the key habits consumers must adopt to better protect themselves from scams.

BNM will also explore stronger protection for vulnerable consumers. This includes assessing whether expanding SEFT's scope would help address the risks faced by this group, while accounting for the level of digital financial literacy and fraud landscape in Malaysia. At the same time, BNM recognises that potential behavioural changes from this expansion could unintentionally compromise customer vigilance. This initiative forms part of multi-pronged efforts to combat fraud and preserve trust in our financial system.

The approach taken in other countries where telecommunication service providers and digital platforms are covered in their compensation frameworks also gives us additional frontiers to consider. Given the critical role of these players in the digital ecosystem, there is merit for Malaysia to consider broadening participation in fraud compensation to further strengthen consumer protection and uphold accountability across all parties.

---

[4] Affected customers may reach FMOS via their portal here: (*https://complaint.fmos.org.my/index.php*).

[5] These refer to cases where victims are deceived into transferring money to fraudsters under false pretences. Here, fraudsters use social engineering tactics to exploit emotions like greed, fear, or love, making individuals vulnerable to fraud.

Diagram 3: Protecting Oneself from Scams

Source: Bank Negara Malaysia