Building a United Front Against Online Fraud Risk

Did you know that ...

1. **Online fraud is a global threat, affecting both individuals and businesses.**
   Globally, one in five consumers have fallen victim to fraud in the last four years.[1]

2. **Scammers and fraudsters target people from all walks of life.**
   No one person or group of people is immune to online fraud. In fact, working adults are the primary target for scams in Malaysia given their perceived wealth.

3. **In 95% of scams in Malaysia, victims knowingly transfer money to scammers.**
   Scammers rely on different tactics to deceive their victims into sending them money. These are known as authorised fraud.[2]

[1] Source: ACI Worldwide
[2] Source: Polis Diraja Malaysia (PDRM)

Aishah, enticed by the promise of high returns, transfers her entire savings to a purported investment company on the advice of her friend. Despite constant reminders about investment scams from her bank and family, Aishah believes that the investment scheme is legitimate. Aishah later finds out that the investment is indeed a scam, and she loses all her money.

Adam receives a digital wedding invitation from a friend. He clicks the link to confirm his attendance. Later that night, he is shocked to discover several large fund transfers were made without his knowledge. He suspects the link was the cause of this as it may have triggered the installation of a malicious app.

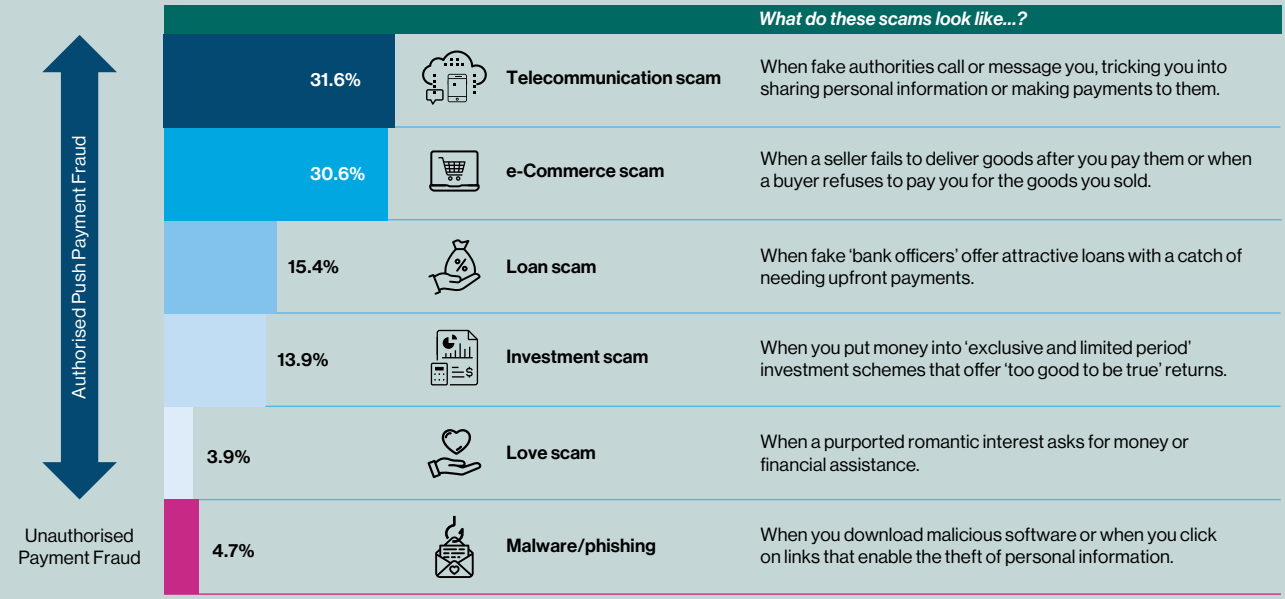
Stories like these have become common but there is a key distinction between these two situations. This lies in the element of customer consent which helps distinguish between the two broad types of fraud – authorised and unauthorised fraud (Diagram 1).

- Aishah's story depicts how an authorised fraud occurs. Victims are deceived into knowingly transferring money to fraudsters under false pretences. These fraudsters use social engineering tactics to exploit emotions like greed, fear or love, making individuals vulnerable to fraud.

- Meanwhile, Adam experiences an unauthorised fraud which involves transactions made by fraudsters without the victim's knowledge. Fraudsters use methods like malware and phishing to obtain personal credentials of their victims. Once these credentials are obtained, fraudsters perform transactions without the victim's knowledge.

Online fraud, be it authorised or unauthorised, is a global threat that affects individuals of all ages and educational backgrounds, and even businesses. This raises an important question: how can we collectively strengthen our defences against fraud and minimise its harm so that stories like the ones of Aishah and Adam become few and far between?

Diagram 1: Main Scam Cases Reported to Polis Diraja Malaysia (PDRM)

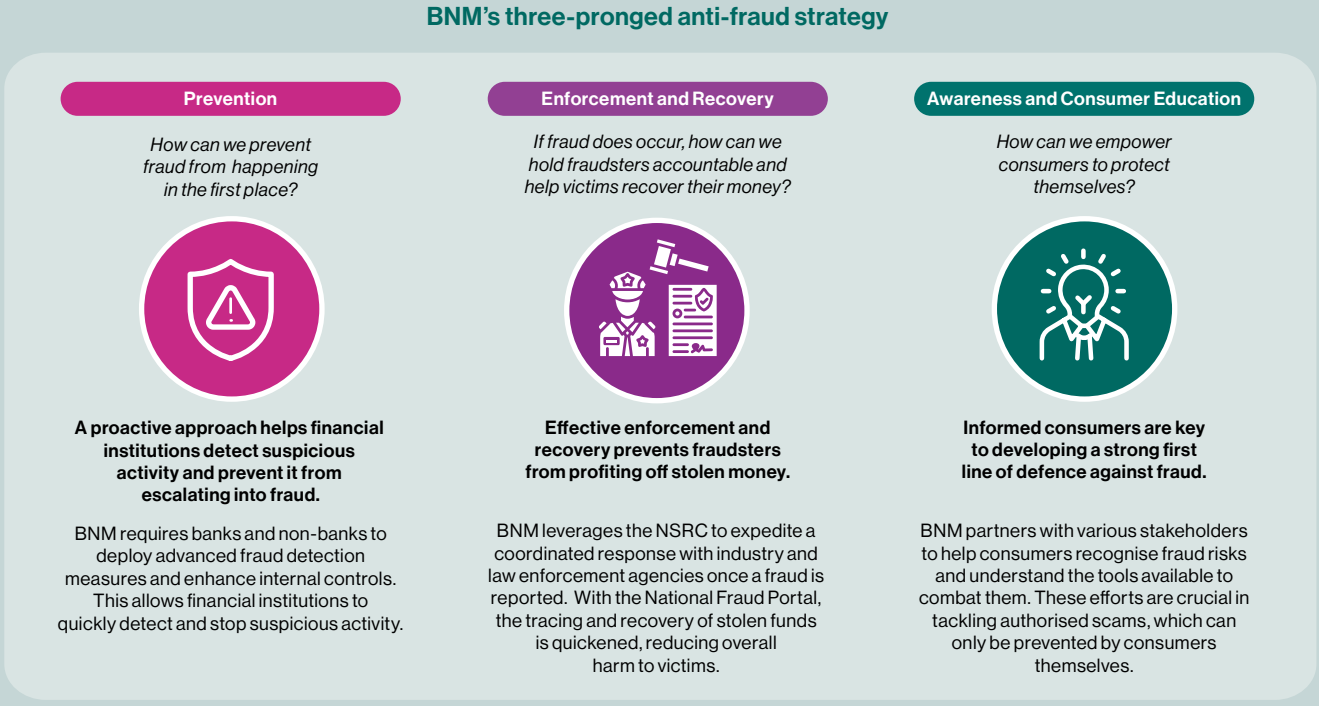


Source: Polis Diraja Malaysia (PDRM)

Multi-pronged approach to strengthen resilience

Malaysia recognised that combatting the threat of fraud requires a multi-pronged approach. A host of measures surrounding prevention, enforcement and awareness is essential to establish a robust defence against online financial fraud (Diagram 2). Importantly, for these measures to be effective, it calls for everyone to work together.

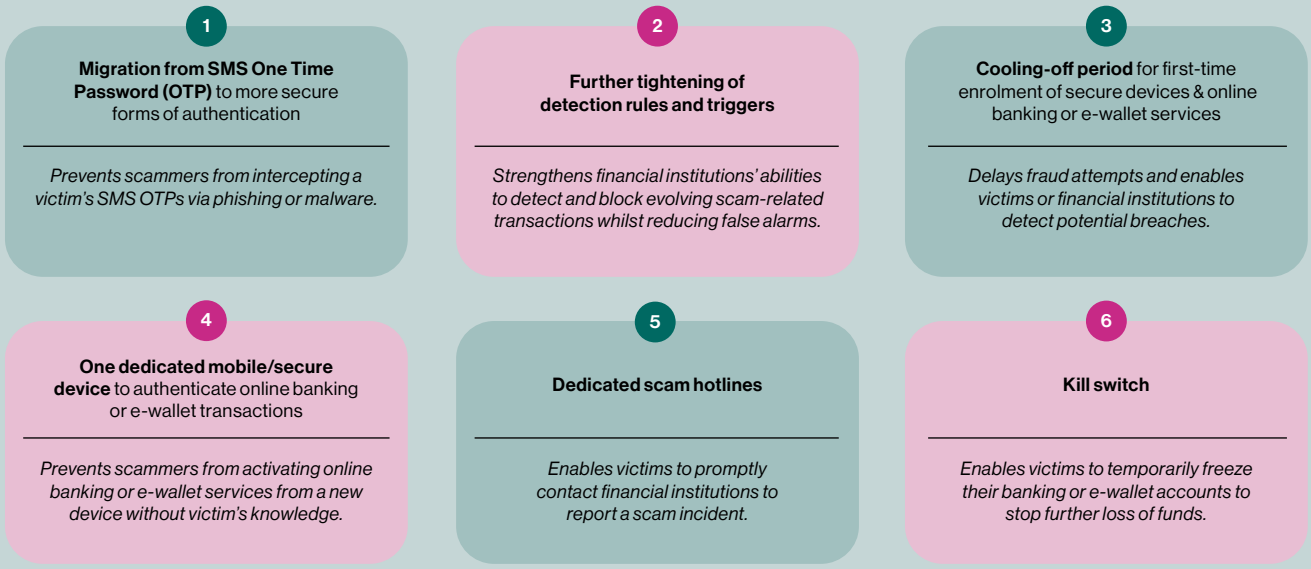
Diagram 2: Understanding BNM's Three-pronged Anti-fraud Strategy



Source: Bank Negara Malaysia

Malaysia has advanced our fight against online fraud. Since 2022, concerted efforts have been undertaken to strengthen security controls of our financial institutions to prevent fraud (Diagram 3).[1] These preventive measures, which have been implemented by all banks and recently extended to all major e-money issuers, have yielded positive outcomes. In 2024, the number of cases of fraudulent unauthorised transactions involving malware and phishing reported to BNM declined by 52%. With these enhanced security controls, the banking industry also managed to avert over RM399 million in attempted fraudulent transactions in 2024. The amount is five times larger than the actual total losses from online fraud transactions reported to BNM.

Diagram 3: Security Measures Implemented by Financial Institutions



Source: Bank Negara Malaysia

On enforcement, the National Fraud Portal (NFP)[2] went live in April 2024 to support the operations of our National Scam Response Centre (NSRC). NSRC acts as a primary contact point for victims to quickly lodge reports of fraud. NSRC officers use the NFP as a platform for tracing the flow of fraud transactions, sharing information among financial institutions and monitoring the intervention actions taken by financial institutions. This has resulted in a 75% reduction in the time taken to obtain complete information on fund flow and a 41% increase in cases being escalated to PDRM for further investigation.[3]

Vigilant and proactive consumers is key to minimising fraud

In Malaysia, more than 95% of online fraud are due to authorised transactions. As the pattern of authorised fraud can closely resemble genuine transactions, financial institutions face significant challenges in identifying and blocking fraudulent transactions without risking disruptions to the smooth functioning of the payment system. Rather, the best way to prevent these transactions from happening in the first place is to educate and increase consumers' awareness on such scams. This is where BNM, government agencies, and the financial industry have intensified their efforts. Greater success in averting fraud can only be achieved if consumers take proactive actions to safeguard themselves from fraud. These include resisting deals that are 'too good to be true', taking heed of scam warnings from friends, family and banks, as well as practising good cyber hygiene by not sharing passwords, personal credentials and not clicking suspicious links.[4]

[1] Refer to Diagram 6 titled 'Three-pronged Approach to Combatting Financial Fraud and Scams' in Annual Report 2023 for further details on the fraud countermeasures within BNM's anti-fraud strategy (https://www.bnm.gov.my/documents/20124/12142010/ar2023_en_ch1e.pdf).

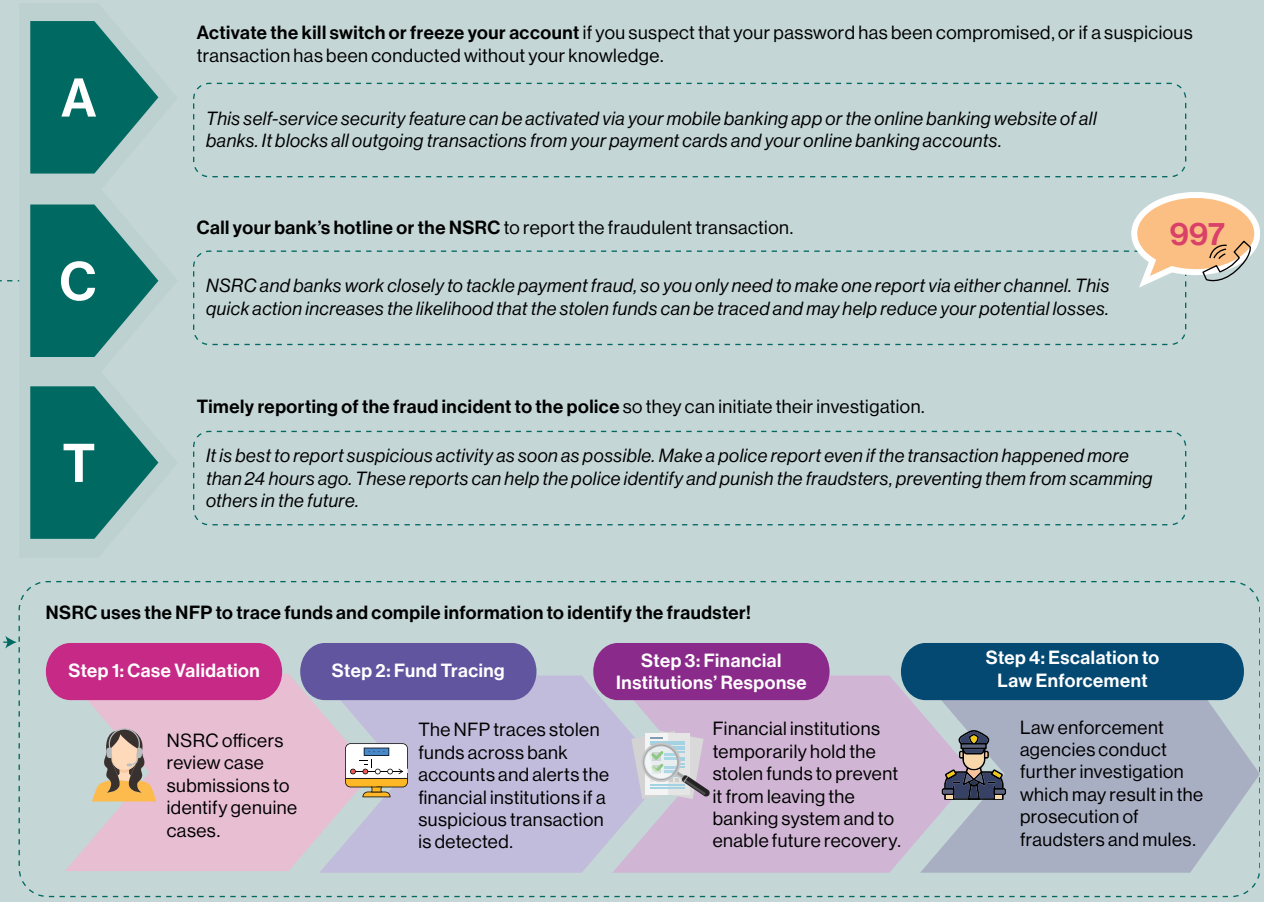
[2] Refer to Diagram 3 of 'Maintaining Financial Integrity' chapter in Annual Report 2023 (https://www.bnm.gov.my/documents/20124/12142010/ar2023_en_ch1g.pdf)

[3] Refer to 'Maintaining Financial Integrity' chapter in Annual Report 2024 for further details on developments related to the NFP. https://www.bnm.gov.my/ar24ch1g.

[4] Based on the Financial Capability and Inclusion Demand Survey conducted in 2024, 15% of respondents willingly shared their banking passwords with close friends, 61% do not pay attention to security features of the banking websites they use, while 80% do not change their passwords regularly.

That said, if consumers still fall victim to fraud, prompt ACTion by consumers is key (Diagram 4). It will help financial institutions and enforcement agencies to respond swiftly and minimise further losses. It also supports efforts to prosecute the perpetrators.

Diagram 4: Swift ACTion by Consumers Can Minimise Fraud Losses



Source: Bank Negara Malaysia

Fair treatment for victims of unauthorised transactions

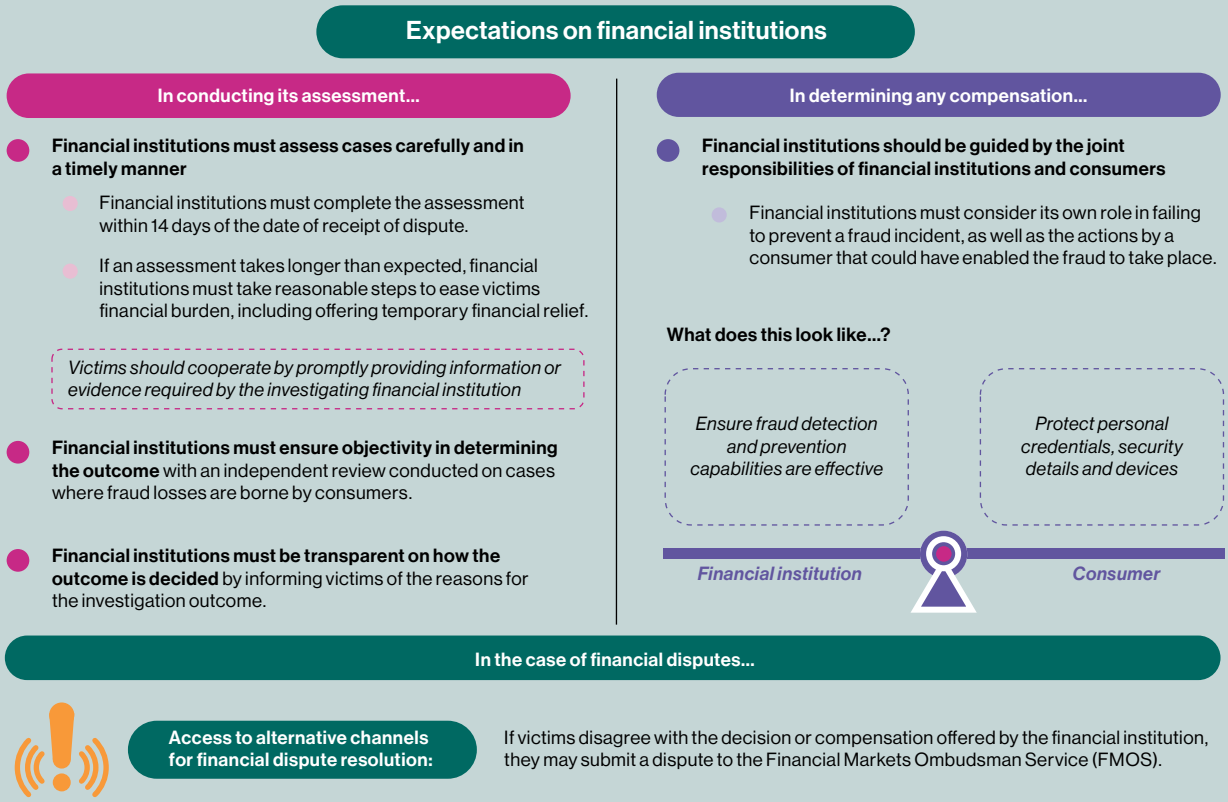
Consumers reasonably expect financial institutions to safeguard their funds. Likewise, financial institutions depend on consumers to be alert and careful to avoid falling victim to fraud. Therefore, both financial institutions and consumers have a shared responsibility to keep bank accounts secure. In line with this shared responsibility, BNM has issued a policy on Ensuring Fair Treatment to Victims of Unauthorised e-Banking Transactions to banking institutions in 2024. Diagram 5 provides an overview of the policy which aims to ensure that investigations by financial institutions into unauthorised fraud incidents and compensation to victims are fair and equitable. Let's look back to the cases relating to Aishah and Adam.

In Adam's case, both Adam and his bank are jointly responsible for enabling the fraud to occur. Adam should have verified the link before clicking on it. Nonetheless, the bank should have paused the transaction and alerted Adam once it detected a series of large and rapid fund transfers to a new third-party individual late at night which is not Adam's typical banking transaction behaviour. Hence, the bank must consider both parties' failure to take reasonable steps to prevent this fraud in determining the compensation to Adam.

Meanwhile, for Aishah who willingly transferred the money given the attraction of the high investment returns, any recovery of the stolen funds will depend on her taking prompt ACTion. Empowering customers through education is the best measure to reduce such fraud.

Recognising red flags before transferring funds can save consumers from losing their hard-earned money. Heed financial institutions' warning on potential fraud to avoid falling prey to scams. Ongoing education and awareness can empower consumers to remain vigilant and protect themselves from scams, especially in cases like Aishah's.

Diagram 5: Overview of the Expectations on the Financial Institutions



Source: Bank Negara Malaysia

Looking ahead

The fight against online fraud is an ongoing challenge and requires a whole-of-nation approach. In this fight, BNM is committed to constantly enhance our strategy by ensuring financial institutions implement strong fraud prevention measures, improving the efficiency and effectiveness of the investigation and enforcement process, and increasing consumer awareness and protection.

The industry is already taking steps to bolster current efforts. This includes exploring ways to continuously strengthen fraud prevention and enforcement through greater use of technology and information sharing.

All of us, as consumers, play a vital role in combatting fraud. As the first line of defence, consumers can help prevent fraud and contribute to a safer digital payment ecosystem by staying vigilant and proactive. Only collectively can we enhance our resilience against this financial threat.