Scam victim's successful bid sets precedent for banks

PETALING JAYA: A landmark court ruling ordering a bank to compensate a scam victim RM166,000 for losses incurred through unauthorised online transactions could set a precedent for greater accountability among banks.

The victim's lawyers said their client, a housewife in her 30s, succeeded in her claim after the court found that account withdrawals in 2021 were made without her consent.

Lawyer K. Revathi said the Kuala Lumpur Sessions Court found inconsistencies between one-time-password (OTP) records submitted by the bank and phone records from the client's telecommunications provider, while some transactions allegedly did not trigger SMS notifications.

"The judge also ruled that the unusual transaction pattern should have raised red flags for the bank. Several mule account holders linked to the transfers, later arrested by police, pleaded guilty in separate criminal cases," she said yesterday.

The ruling is believed to be the first case in Malaysia where a scam victim succeeded in challenging unauthorised online banking transactions.

Revathi said the legal team referred to an Indian Supreme Court judgment involving a bank and a defrauded customer to support its arguments that the transactions were fraudulent.

Co-counsel K. Gunalan said the suit was filed after attempts to resolve the matter through mediation in 2021 failed.

"The judge also ruled that the bank had the technical capability to detect suspicious transactions and should have identified the red flags when the unusual withdrawals took place.

"Our client rarely carried out online banking transactions, preferring over-the-counter dealings and did not even have the bank's application installed on her smartphone," he said.

Revathi said further investigations should have been carried out to determine how her client's bank account could have been compromised.

Meanwhile, lawyer Thulasy Suppiah, who specialises in cases involving artificial intelligence (AI) and cybersecurity, said banks could no longer rely on the argument that their systems were not technically breached, especially as modern scams increasingly use AI and social engineering to manipulate victims into authorising transfers themselves.

"Scammers do not necessarily hack into a bank's systems. Instead, they manipulate people into approving the payment.

"Because of this, banks now have a growing legal duty to implement behavioural monitoring systems capable of detecting unusual transactions even if an OTP or TAC was technically entered," she said.

"AI scams work differently as they deceive employees or customers into authorising what appears to be a legitimate transfer."

She said banks should redesign their internal approval systems to include independent verification measures for high-risk transactions.

Thulasy also said the landmark ruling could potentially open the door for more scam victims to pursue legal action over unauthorised withdrawals.

"This ruling establishes that technical security measures alone are no longer a complete defence if obvious red flags were ignored," she said.