EXPERT**SPEAK**

Should you be held responsible for preventing e-wallet fraud?

One of the latest victims of cyber fraud is Ambience Mall's general manager Arvind Kapoor, who lost ₹1.85 lakh to a fraudster posing as a Paytm employee. Even as fraudsters invent new ways to dupe customers and wallet providers struggle to plug the leaks, there is some ambiguity about who should take the fall in case a fraud occurs. While the Reserve Bank of India's (RBI) mandate holds the provider responsible if the negligence is at their end and the customer liable if they give out sensitive information, it's not always black and white. Nilanjana Chakraborty spoke to experts to find out how incidences of fraud are handled

BHARAT PANCHAL
Chief risk officer, India, Middle East and Africa, Fidelity National Information Services

Customers need to be equally responsible

In recent years, cases of fraud linked to Netbanking and mobile wallets have increased significantly. It's largely seen that customers share their credentials with fraudsters either out of fear or greed. Indian customers don't have adequate awareness about safe usage.

Though cases of fraud have increased, a large number of banks have still not enhanced their infrastructure to detect or prevent fraud from the system. Real-time fraud detection using artificial intelligence and machine learning are highly recommended technologies. But banks have still not geared up to adopt such advanced tools.

The biggest modus operandi used by fraudsters is social engineering in which customers fall prey and give out sensitive information. It's very difficult to catch fraudulent transactions that have been made using genuine credentials shared by the customers.

Banks are responsible to provide safe banking, while customers are responsible to ensure that any sensitive details are not shared with anyone. Technology has a solution for everything but sadly it cannot solve human behavioural issues.

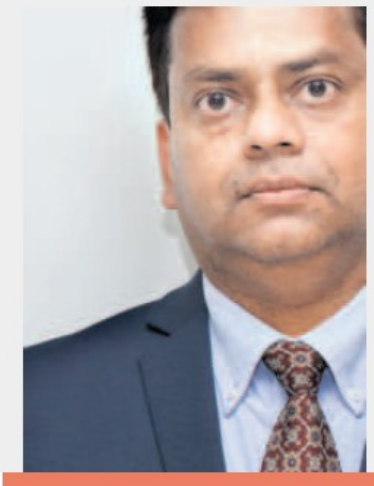
RAJESH MIRJANKAR
Managing director and chief executive officer, InfrasoftTech

Wallets must have AI-based anti-fraud solutions

Phishing is the most common type of fraud for wallets and online transactions. The common modus operandi is—the customer receives a call, SMS or email from a fraudster claiming to be from the wallet firm either to confirm KYC details or to receive and encash offers. Frauds can also occur when victims click on links that could download trojans on phones, leading to siphoning off funds from wallets.

Customers should never provide login credentials or other details on email. Mobile users should not click on any images or links from unknown sources on SMS or any messaging app. In case of a fraud, report it to the wallet firm and get it blocked to prevent further losses. Simultaneously, report the incident to the police or the cyber crime cell.

To combat frauds, wallet companies are mandated to provide frequent reminders to users to not respond to random emails. They must highlight the correct modes of approaching the firm. They must implement AI-based, anti-fraud solutions to prevent fraud. They must also implement cyber security tools to prevent trojan attacks.



MICHAEL JOSEPH
Director, system engineering, India and SAARC, Fortinet

Providers need to keep pace with modern cyber attacks

Making a mobile payment involves a device, a merchant, a POS system, financial institutions that process the payments, and organizations that provide services to the consumer. Inadequate security measures at any of these stages can put users at risk.

Compromising mobile devices not only allows attackers to steal data stored on the device but can be used to collect personal banking information using phishing apps, intercept data moving between a user and the bank, and monitor financial transactions. Given the hyper-connected ecosystem of devices, applications and data in which financial services now exist, it is important that they deploy and use interconnected security features and solutions.

Users are rapidly adopting mobile payments and are expecting banks and financial services firms to ensure their security. Hence, financial service providers and fintechs must increase their ability to leverage security features across distributed environments to keep pace with modern, automated cyber attacks and protect mobile payment users.

ANAND KUMAR BAJAJ
Managing director and chief executive officer, PayNearby

More detection tools needed, but users need to be careful

RBI has taken several measures to control these frauds such as asking e-wallet companies to set up 24x7 customer care helplines to report fraud and offer customer assistance at the hour of need.

A customer-centric approach to ensure prevention of frauds puts a lot of ownership on the issuer. Companies must invest in fraud detection software to mitigate risk, be PCI-DSS compliant and have robust transaction monitoring systems. Companies should make consumers aware of the risks involved, and educate them against fraudulent measures.

Consumers need to be aware against sharing confidential data, especially through methods like phishing, where sensitive information is stolen through innocuous emails or WhatsApp messages. Consumers should be mindful that bank officials or wallet companies will never ask for confidential details. To be on the safe side, consumers should not park all their funds in one account. Simple steps like setting up SMS and email alerts every time money is deducted from wallets will go a long way.