THINKHOWE

Consumer Attitudes Toward Fraud and Opportunities for Mobile Network Operators in SEA

November 2024

Consumer Attitudes Toward Fraud and Opportunities for Mobile Network Operators in SEA

In today's rapidly evolving digital landscape, financial fraud is a major concern for consumers, financial institutions, and digital commerce providers. Southeast Asia (SEA) is a region where mobile usage, digital transactions, and fintech adoption are growing rapidly, making security and fraud prevention crucial topics of interest for both consumers and businesses. This report focuses on consumer attitudes towards fraud across five SEA markets (Thailand, Singapore, Malaysia, Indonesia, and the Philippines) and explores the opportunities for mobile network operators (MNOs) to develop and implement APIs that can assist fintech and digital commerce providers in addressing these security concerns.

The study draws on data from a consumer survey on perceptions, preferences, and concerns related to key API features and use cases that have been developed to be made available with the GSMA OpenGateway project. The initial findings indicate that consumers across these markets share a growing concern about fraud, especially in financial transactions, and there are clear opportunities for MNOs to step in as key players in providing secure mobile services through API-driven solutions.

1. Consumer Attitudes Toward Fraud in Southeast Asia

1.1 Overview of Consumer Concerns

Fraud, particularly in financial transactions, has emerged as one of the foremost concerns among consumers in Southeast Asia. The data indicates a clear trend of increasing anxiety about security risks, with more than half of the respondents across all markets expressing concern about the rising likelihood of fraud and hacking. These concerns are particularly pronounced in Indonesia and Malaysia, where nearly **43%** and **34%** of respondents, respectively, said they were "very worried" about becoming a victim of fraud.

Furthermore, financial fraud, such as account hacking, SIM-swap attacks, and stolen credit card information, has been a common experience in several markets. Singapore and Malaysia report the highest levels of direct fraud experience, with over 30% of respondents having encountered financial fraud at least once. In contrast, Thailand and Indonesia report lower but still significant levels of fraud experiences, with around 20-26% of respondents indicating that they have been affected.

Consumers are acutely aware that the increasing digitisation of financial services comes with greater security risks. This growing perception of vulnerability is shared across the region, with 50-57% of respondents in most markets stating that they believe account security risks are “going up,” and 14-20% of respondents noting that they believe these risks are “increasing rapidly.”

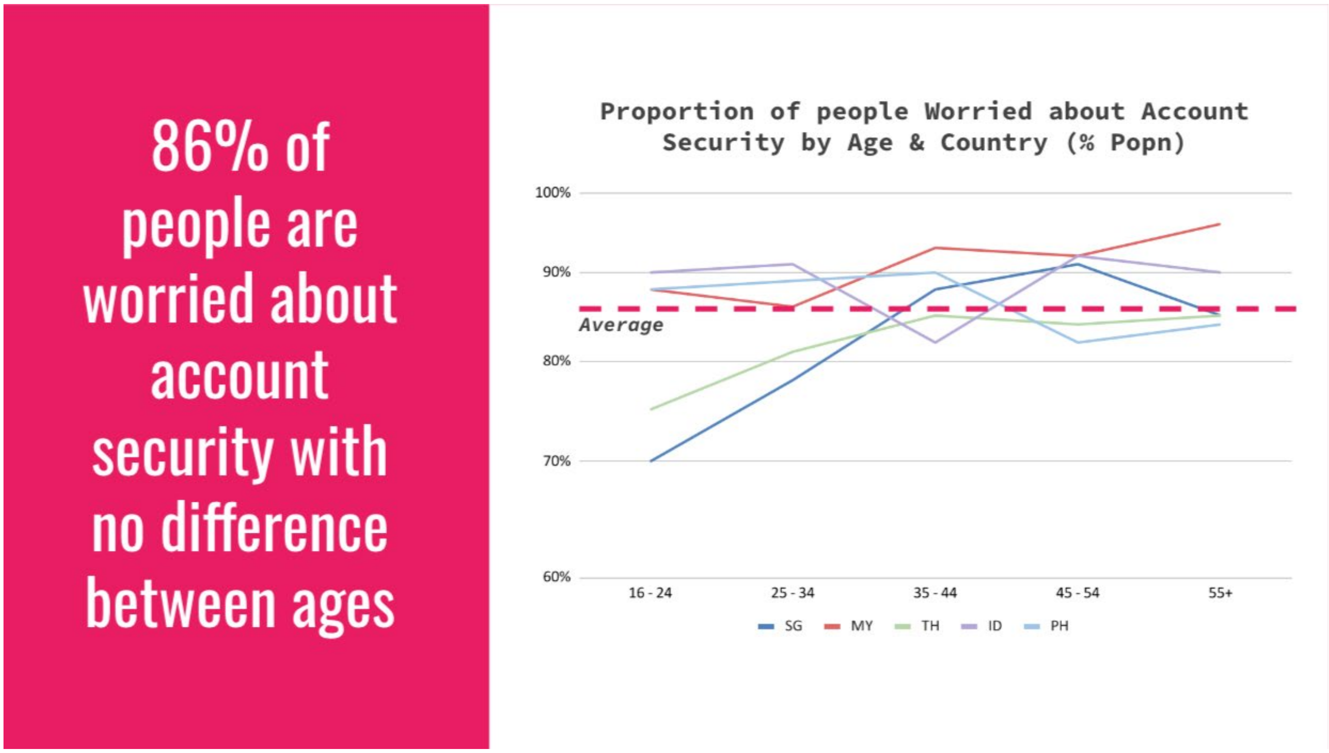
1.2 Key Fraud Concerns

Consumers’ concerns about fraud in SEA tend to focus on a few key areas, such as:

SIM-Swap Attacks: This type of fraud, in which a hacker gains control of a mobile number by transferring it to a new SIM card, is a significant worry in several markets. Indonesia (78%) and the Philippines (71%) report the highest levels of concern about SIM-swap fraud, while Singapore, though relatively more secure, still sees 50% of consumers highly concerned.

Mobile Payments and E-Wallets: With the increasing adoption of mobile wallets and digital payments across SEA, many consumers are worried about the potential vulnerabilities of these platforms. Malaysia (75%) and Indonesia (91%) show particularly high adoption rates of e-wallets, and with that comes heightened concern of consumers about fraud.

Personal Data Theft: Across all five markets, consumers expressed serious concerns about the protection of their financial data. More than 60% of respondents in Malaysia, Indonesia, and the Philippines are very worried about the misuse or theft of Personally Identifiable Information (PII) and financial data. These concerns are rooted in the growing number of high-profile data breaches across the region.



1.3 Responsibility for Security

When asked who is most responsible for preventing fraud and ensuring security, respondents across all five markets overwhelmingly pointed to account custodians (i.e., banks, e-wallet providers, etc.). Between 43% (Malaysia) and 62% (Indonesia) of respondents assigned primary responsibility to the companies operating the services. This places fintech companies, banks, and other financial institutions at the forefront of fraud prevention efforts.

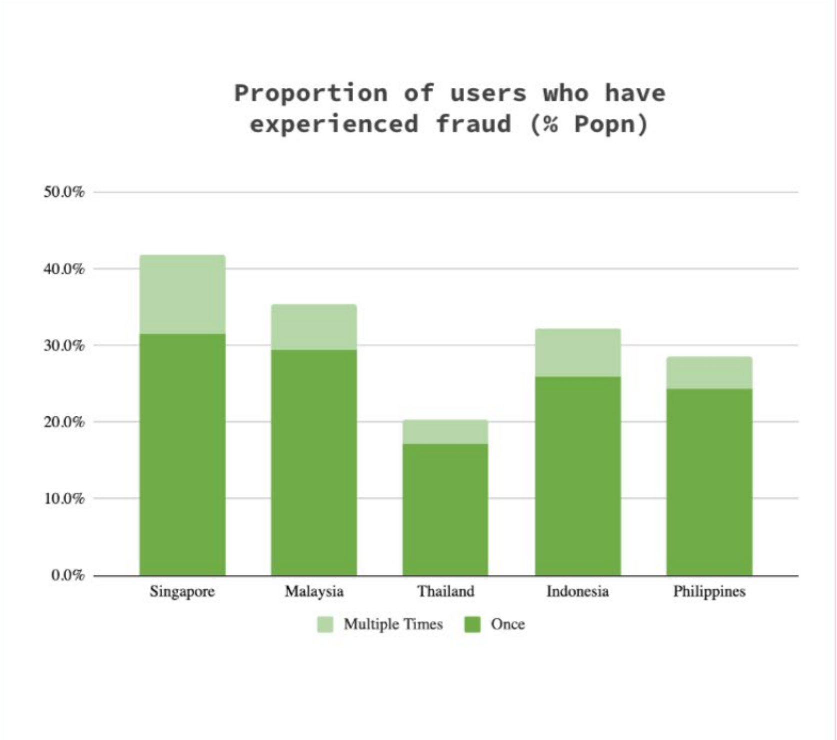
However, consumers also expect device manufacturers (such as Apple, Google, and Samsung) to play a key role in protecting their accounts. This expectation is higher in markets like the Philippines, where 29% of respondents believe that device manufacturers bear some responsibility, compared to 15% in Indonesia.

MNOs and Government expectations in this area were fairly consistent with around 10%-13% of participants across all markets expecting some responsibility to be born for each of these organisations.

2. Opportunities for Mobile Network Operators (MNOs) to Address Fraud Through API Development

MNOs in Southeast Asia are uniquely positioned to address the growing concerns about fraud. By developing APIs that integrate with fintech platforms, banks, and digital commerce providers, MNOs can offer enhanced security features, real-time fraud detection, and data-sharing tools that can help protect consumers from various forms of fraud.

In Singapore 42% of people have already been a victim of fraud



2.1 API Opportunities for Enhanced Account Security

One of the most significant opportunities for MNOs lies in the development of APIs that strengthen account security and prevent fraudulent activities like SIM-swap attacks. The high level of concern surrounding these attacks, particularly in markets like Indonesia and the Philippines, makes this an area of urgent need.

2.1.1 Two-Factor Authentication (2FA) APIs

Two-factor authentication (2FA) is one of the most widely adopted security measures across all markets, with 66% of respondents in Singapore and 51% in Thailand identifying it as a key security feature. MNOs can enable 2FA APIs that fintechs and digital commerce providers can integrate more seamlessly into their platforms. These APIs allow consumers to receive real-time verification codes via SMS or push notifications, adding an additional layer of security to sensitive transactions.

Opportunity: MNOs can partner with fintechs to integrate 2FA directly into mobile banking apps, e-wallets, and digital commerce platforms (Silent OTP), creating a seamless user experience where the mobile network serves as an authentication tool. Given the wide adoption of 2FA in Singapore and Malaysia, these markets could be early adopters of such solutions.

2.1.2 SIM-Swap Fraud Detection APIs

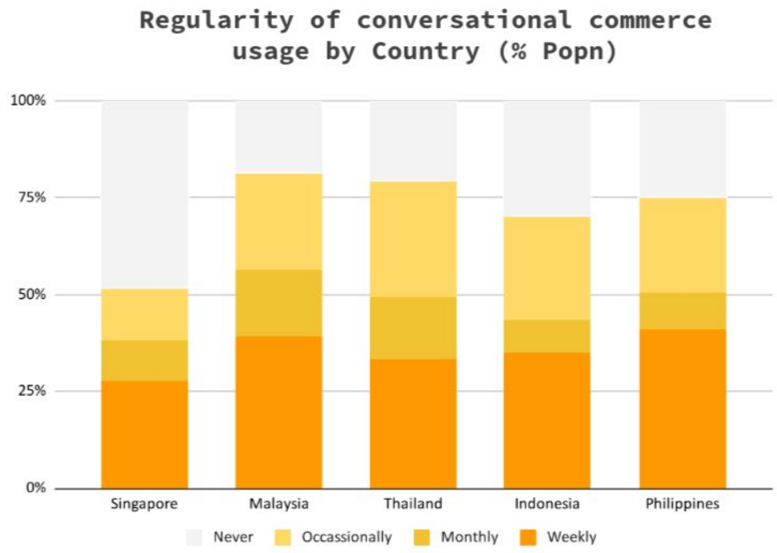
In markets like Indonesia and the Philippines, where SIM-swap fraud is a major concern, MNOs can develop APIs that provide real-time monitoring and alerts for SIM changes. These APIs would notify fintech platforms if a user’s SIM card has been swapped, allowing them to take preventive actions, such as temporarily locking accounts or requiring additional authentication steps. SIM-Swap attacks are particularly prevalent with cryptocurrency hacks as there is little to no chance of recalling funds once they have been sent from the account.

Opportunity: MNOs can offer SIM-swap detection as an add-on service for fintechs and banks, creating a business model based on protecting high-risk transactions. This would be particularly valuable in Indonesia and the Philippines, where SIM-swap fraud is perceived as a critical issue.

2.2 APIs for Fraud Prevention in Digital Commerce

Digital commerce is booming in Southeast Asia, with platforms like WhatsApp, TikTok, and Facebook Messenger becoming key channels for online purchases. However, with the rise of social commerce comes the risk of fraudulent transactions. MNOs can play a pivotal role in securing these platforms by developing fraud prevention APIs that integrate directly with digital commerce providers.

77% of Thai users make purchases through conversational apps



2.2.1 Real-Time Transaction Verification APIs

One of the most effective ways to prevent fraud in digital commerce is through real-time transaction verification. MNOs can create APIs that allow digital commerce platforms to verify the authenticity of a transaction by cross-referencing the user's mobile number, location data, and transaction history.

Opportunity: In markets like Thailand and Malaysia, where social commerce is thriving (with 77% and 62% of consumers making purchases through apps like WhatsApp), MNOs can offer real-time verification services to ensure that user accounts are legitimate and reduce fraud risk for consumers and merchants.

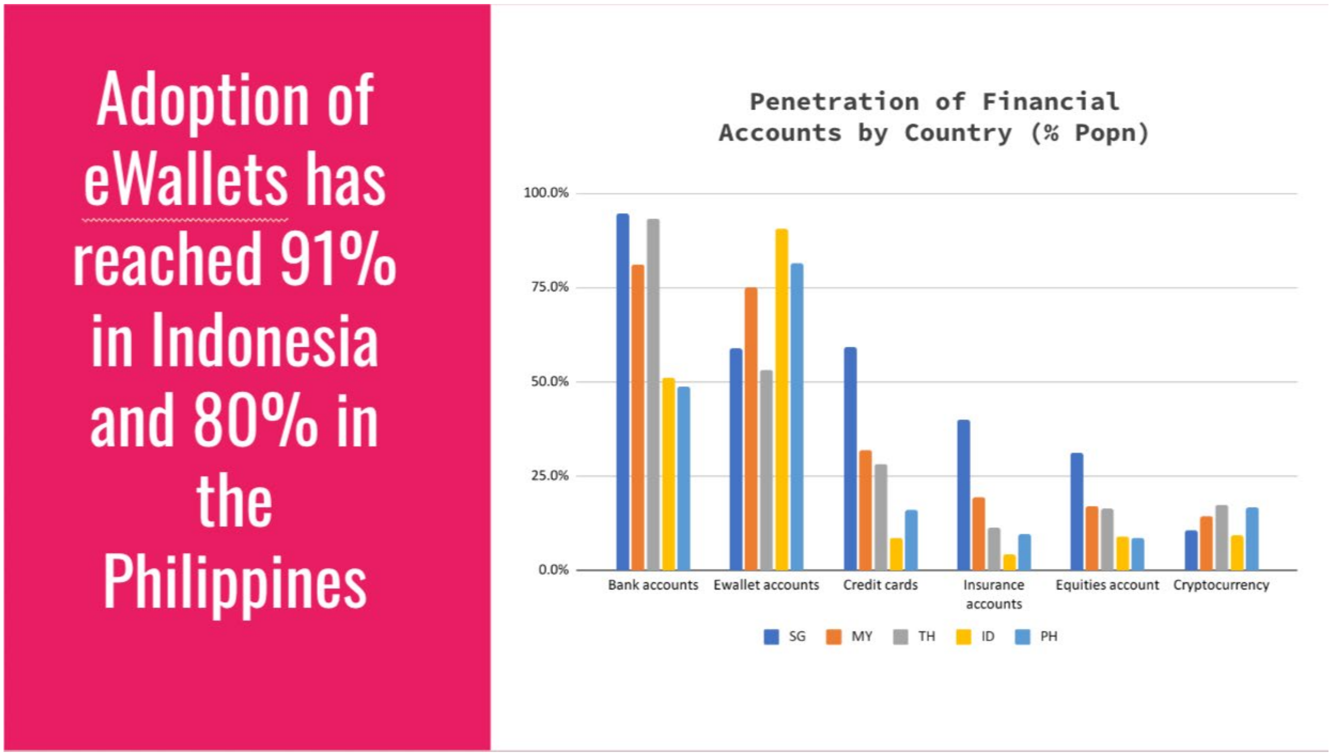
2.2.2 Location-Based Fraud Detection APIs

MNOs have access to vast amounts of user data, including real-time location information. By developing APIs that provide location-based fraud detection, MNOs can help fintechs and digital commerce platforms verify if a transaction is being made from a suspicious or unexpected location.

Opportunity: In Malaysia and Indonesia, where consumers are more open to sharing location data to prevent fraud, MNOs can collaborate with digital commerce platforms to provide location-based security features. This would reduce fraudulent transactions on social media commerce platforms by verifying if the user's location matches their purchase behaviour.

2.3 APIs for Mobile-First Financial Services

Given the high penetration of mobile devices across Southeast Asia, with 91% of respondents in Indonesia and 80% in the Philippines accessing their financial accounts via mobile, MNOs are well-positioned to develop APIs that enhance the convenience and security of mobile-first financial services.



Adoption of eWallets has reached 91% in Indonesia and 80% in the Philippines

2.3.1 E-Wallet Integration APIs

The widespread use of e-wallets in markets like Indonesia and the Philippines presents a significant opportunity for MNOs to develop APIs that integrate mobile services with e-wallet platforms. These APIs would provide fintech and other industries seamless identity verification, transaction monitoring, and secure fund transfers.

Opportunity: MNOs can develop APIs that are part of the value chain to enable real-time balance checks, instant fund transfers, and fraud detection within e-wallets, improving the overall user experience while ensuring that transactions remain secure. This could drive further growth in mobile financial services in markets with high e-wallet adoption, such as Indonesia (91%) and Malaysia (75%).

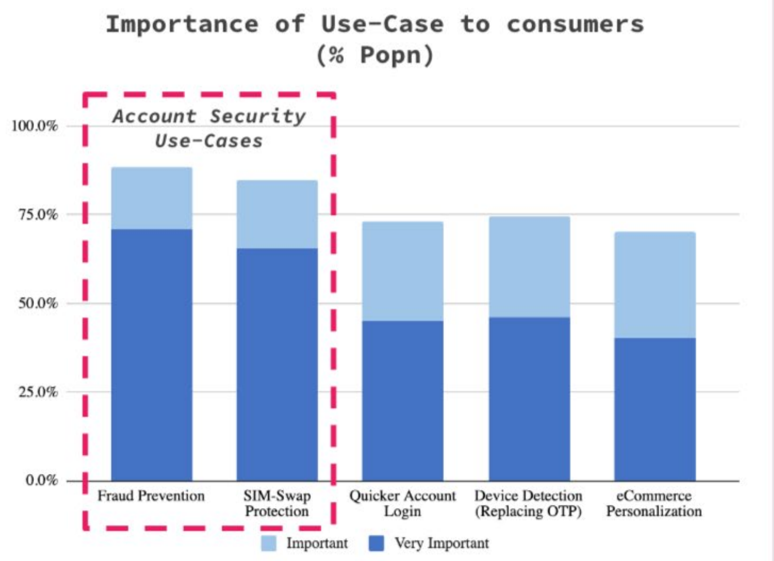
2.3.2 Pre-Filled Information and Mobile Verification APIs

Many consumers in Southeast Asia express interest in pre-filled information when signing up for new services, with 59% of Indonesian respondents indicating that it would make their experience easier.

MNOs can develop APIs that allow fintech and digital commerce providers to automatically verify user information using mobile network provider registration data, such as name, address, and phone number.

Opportunity: This would reduce friction for users signing up for new services, especially in mobile-first markets like Indonesia and Malaysia, where convenience is a key driver for adoption. By offering these APIs, MNOs can streamline onboarding processes for fintechs and e-commerce platforms.

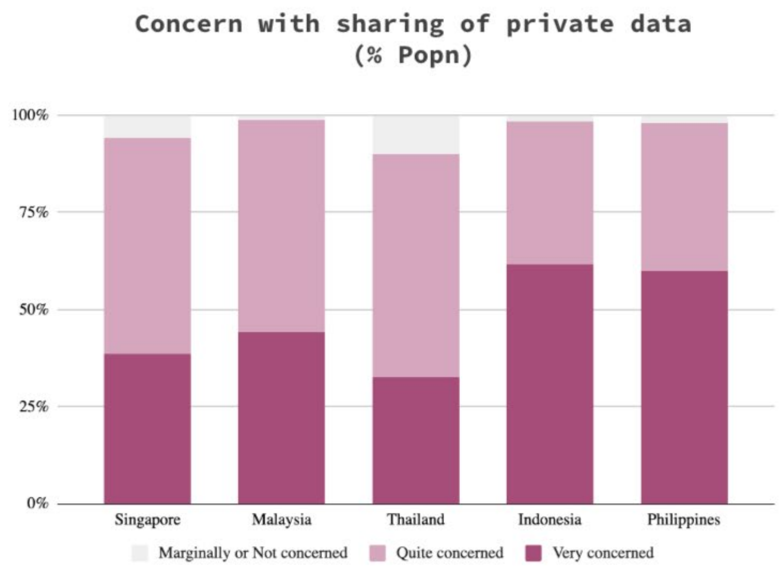
Consumers are looking for higher account security over convenience



3. Regulatory: Privacy Concerns and the Role of MNOs in Offering Transparent Data Solutions

While there is a growing demand for security APIs, privacy concerns remain a significant barrier, particularly in mature markets like Singapore. Consumers are increasingly concerned about how their personal and financial data is used, and many are uncomfortable sharing their information with digital platforms.

Across all countries consumers are concerned about data privacy



3.1 Addressing Data Privacy Concerns

The study reveals that more than 60% of consumers in Indonesia and the Philippines are "very concerned" about data privacy, while 57% of Singaporeans are “quite concerned.” In these markets, consumers are particularly wary about how their personally identifiable information (PII) and financial data are shared, especially with conversational apps like WhatsApp and Facebook Messenger.

MNOs have a critical role to play in addressing these privacy concerns. By developing APIs that prioritize data transparency and user control, MNOs can build trust with consumers while enabling fintech and digital commerce providers to offer more secure services.

3.2 Transparent Data Sharing APIs

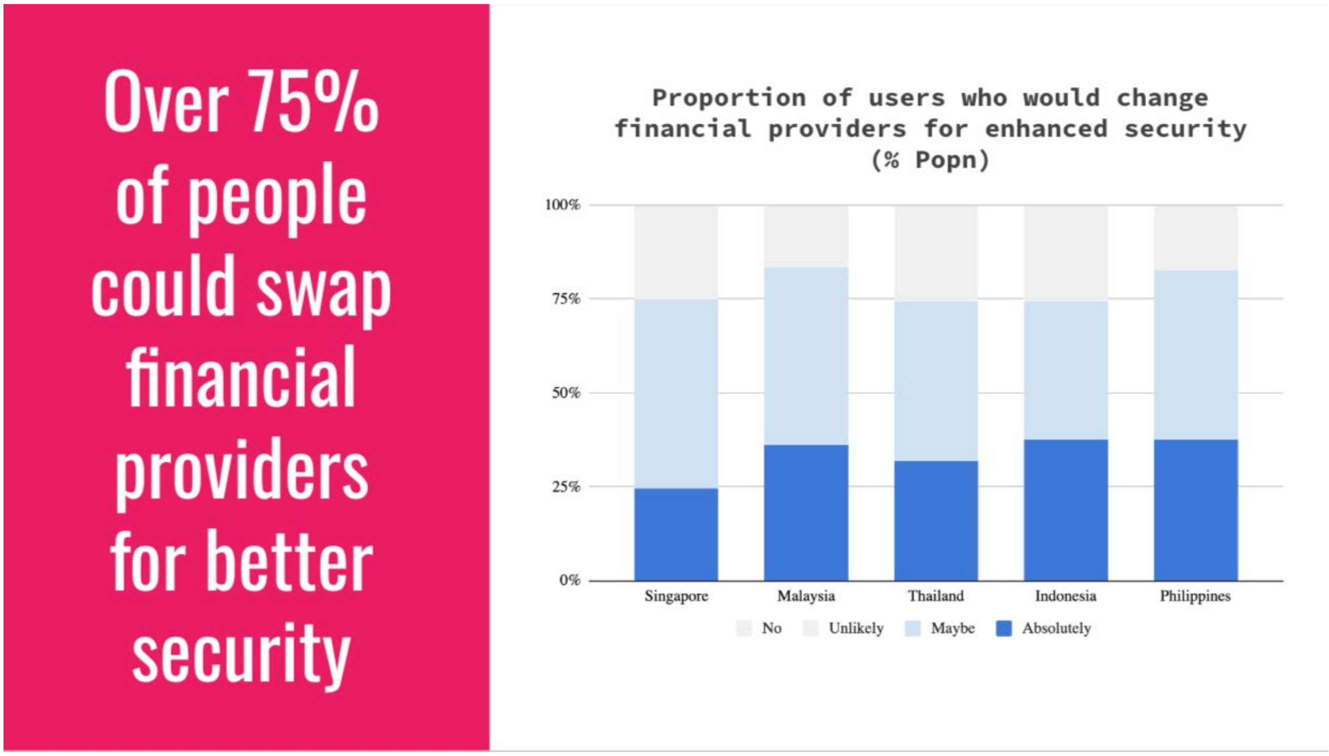
One of the key demands from consumers is transparency about how their data is collected and used. MNOs can develop APIs that allow fintech and e-commerce platforms to disclose exactly what data is being shared and provide users with the option to opt-in or opt-out.

Opportunity: Starting in markets like Singapore, where privacy concerns are higher, MNOs could offer APIs that allow users to manage their data-sharing preferences. This could include options to control which personal information is shared during transactions or interactions with third-party apps.

3.3 Granular Consent Management APIs

Consumers want control over their data. MNOs can develop APIs that offer granular consent management, allowing users to decide exactly what data is shared with each app or service. This would give users greater control over their personal information and address the growing concerns about data misuse in the region.

Opportunity: APIs that enable granular data control would be particularly attractive in privacy-sensitive markets like Singapore and Malaysia, where consumers demand greater transparency from service providers.


Proportion of users who would change financial providers for enhanced security (% Popn)

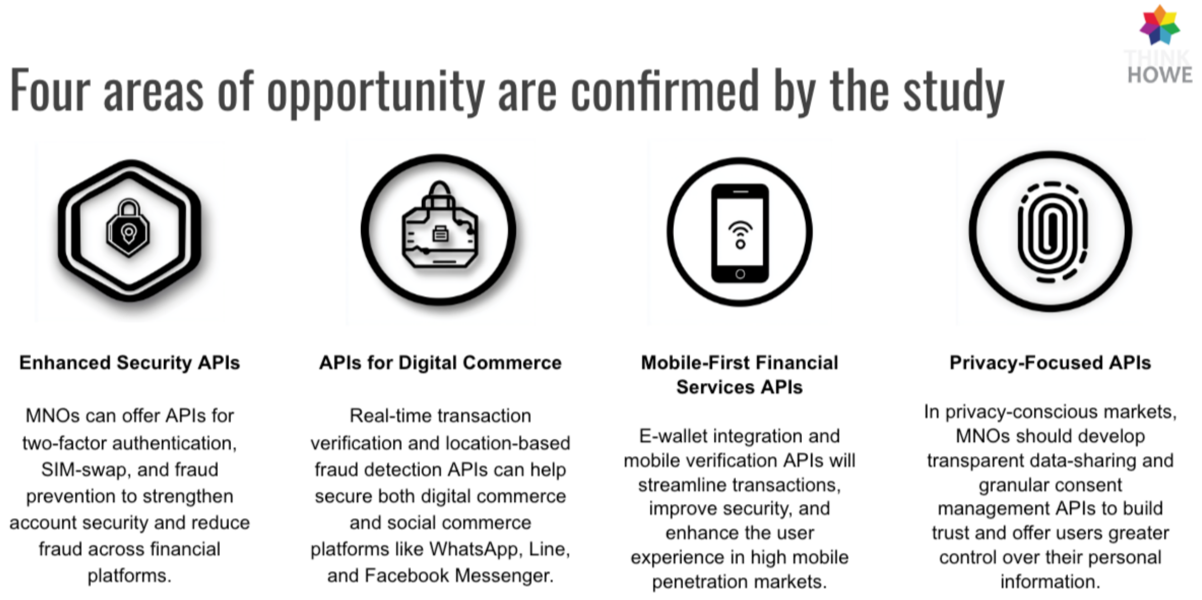
Conclusion: The Path Forward for MNOs in Southeast Asia

The evolving digital landscape of Southeast Asia presents both significant opportunities and challenges for consumers, businesses, and service providers alike. Fraud, particularly within fintech and digital commerce, has emerged as a critical concern, necessitating robust and innovative responses. Mobile Network Operators (MNOs) are uniquely poised to address these challenges, leveraging their technical capabilities and extensive user reach.

This report underscores the urgent need for MNOs to collaborate with fintechs, digital commerce platforms, and governments to establish a secure and trustworthy digital ecosystem. By prioritising the development of targeted API solutions—ranging from fraud detection to enhanced account security and transparent data management—MNOs can play a transformative role in mitigating risks while boosting consumer confidence. The potential for innovative solutions like SIM-swap detection APIs, real-time transaction verification, and granular consent management APIs illustrates the path forward for these operators to not only respond to immediate consumer concerns but also to shape the future of digital commerce in the region.

Equally important is the alignment with privacy expectations, particularly in markets like Singapore and Malaysia, where consumers demand greater transparency and control over their data. Addressing these concerns through APIs that prioritise user consent and data protection will not only help build trust but also ensure compliance with regulatory requirements across diverse markets.

As the digital economy in Southeast Asia continues to grow, MNOs must act decisively. By championing secure, transparent, and user-centric solutions, they have the potential to redefine their role in the digital value chain—from traditional network providers to key enablers of a secure and dynamic digital future. Through partnerships, innovation, and a commitment to addressing consumer concerns, MNOs can catalyse a safer and more inclusive digital economy, setting a benchmark for other regions to follow.



Four areas of opportunity are confirmed by the study

Enhanced Security APIs

MNOs can offer APIs for two-factor authentication, SIM-swap, and fraud prevention to strengthen account security and reduce fraud across financial platforms.

APIs for Digital Commerce

Real-time transaction verification and location-based fraud detection APIs can help secure both digital commerce and social commerce platforms like WhatsApp, Line, and Facebook Messenger.

Mobile-First Financial Services APIs

E-wallet integration and mobile verification APIs will streamline transactions, improve security, and enhance the user experience in high mobile penetration markets.

Privacy-Focused APIs

In privacy-conscious markets, MNOs should develop transparent data-sharing and granular consent management APIs to build trust and offer users greater control over their personal information.

Authors

Tyson Hackwood
Leslie Falvey

17 November 2024

THINKHOWE

Think Howe offers strategy consulting and research services to private companies, governments, and public institutions focused on the Australasian region.

Over the past 15 years, we have worked with clients across the region, creating impact through a combination of outcome focused management and on-the-ground experience.

Email: info@thinkhowe.com