

Zimperium Helps Banks Comply with MAS Mobile Banking Regulations



2023

 ZIMPERIUM[®]

Executive Summary

The mobile banking landscape is facing unprecedented threats, with a steep rise in sophisticated malware attacks undermining the security of mobile applications. Zimperium's extensive research reveals a worrying trend: a 51% increase in unique mobile malware samples from 2021 to 2022. The latest Mobile Banking Heists report shows how 29 banking malware families are targeting 1,800 mobile banking apps. At least 30 of these banking institutions are part of ASEAN.

In response, regulatory bodies globally, including the Monetary Authority of Singapore (MAS), are revising mobile app security guidelines to fortify the digital banking ecosystem. Zimperium's adaptive mobile app security solutions address these challenges, offering dynamic, future-proof protection against growing threats.

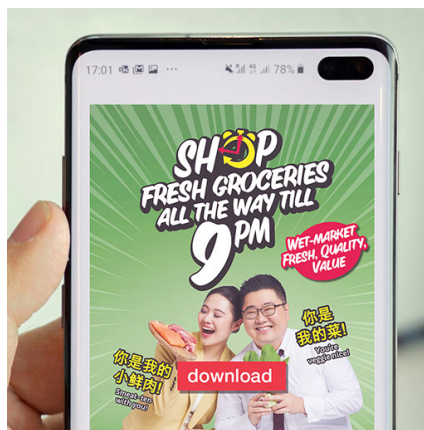
Escalating, Evolving Threats

As financial institutions increasingly pivot towards mobile banking solutions to meet customer demands for convenience and innovation, they encounter a parallel rise in cyber threats. These threats are not static; they evolve continually, becoming more complex and harder to defend against, especially when the app is on the app store and running on end-user devices. This evolution necessitates a proactive approach to mobile app security, ensuring both the safety of corporate assets and the sensitive data of customers and employees.

Recent incidents underscore the urgency of the threat:



There were 22,339 scam cases [reported](#) from January to June 2023, according to mid-year scam statistics from the police, a **64.5% increase** from the 13,576 cases during the same period in 2022.



\$10 Million Lost in Malware Scams (2023): Fraudulent ads on social media have led to significant financial losses, with users [tricked into downloading malicious apps](#).



CPF Savings Theft: Malware accessed via [QR codes and third-party APK downloads](#) resulted in substantial financial losses for individuals in Singapore.



These cases highlight the ingenious methods employed by fraudsters, exploiting the convenience of mobile transactions to their advantage.

The Impact of New Regulation on Foreign and Local Banks

MAS' introduction of Guidelines for Technology and Risk Management can have a significant impact on both local and foreign banks operating in Singapore. Here are some key effects:

- 1. Enhanced Security Standards:** These guidelines likely raise the bar for cybersecurity, data protection, and technology risk management. Banks need to align their systems and processes with these enhanced standards.
- 2. Increased Compliance Costs:** Implementing new technology and risk management practices may result in higher operational costs, especially for smaller banks or foreign banks with less presence in Singapore.
- 3. Competitive Advantage:** Banks that effectively integrate these guidelines could gain a competitive edge in terms of reliability and trustworthiness, which is crucial in the financial sector.
- 4. Innovation Encouragement:** By setting clear technology and risk management standards, MAS may inadvertently encourage banks to innovate and adopt advanced technologies to meet these standards efficiently.
- 5. Global Standard Setting:** As MAS is a respected regulatory authority, its guidelines could influence global standards, affecting how banks worldwide approach technology and risk management.
- 6. Market Entry Barrier:** For foreign banks, these guidelines might increase the barrier to entry into the Singapore market, requiring more substantial initial investments in technology and compliance infrastructure.

In the long run, these guidelines will benefit both the industry and its customers, even though there will be challenges, especially in the short term.

MAS Compliance with Zimperium

Zimperium offers a comprehensive mobile app security suite (MAPS) to address the security requirements outlined by MAS. In order to comply with MAS regulatory requirements for security, Zimperium provides the following capabilities.



Application Shielding

Code protections are applied to strengthen the security of the mobile banking app, making it more resistant to reverse engineering and tampering.



Runtime Visibility and Protection

An in-app security SDK that enables mobile banking apps to defend themselves on end-user devices.













Cryptographic Key Protection

Whitebox protected cryptographic libraries to prevent exfiltration of keys at rest, in motion or in memory.



Mapping to Technology and Risk Management Guidelines

Zimperium Solutions			
ANNEX C: Mobile App Security Requirements	zShield	zDefend	zKeyBox
(a) avoid storing or caching data in the mobile application to mitigate the risk of data compromise on the device. Data should be stored in a protected and trusted area of the mobile device;			
(b) protect private cryptographic keys;			
(c) implement anti-hooking or anti-tampering mechanisms to prevent injection of malicious code that could alter or monitor the behavior of the application at runtime;			
(d) implement appropriate application integrity check			
(f) implement a secure in-app keypad to mitigate against malware that captures keystrokes; and			
(g) implement device binding to protect the software token from being cloned.			
(e) implement certificate or public key pinning to protect against MITMA;			

Enhanced Security Measures Against Malware Scams

Requirements	zDefend Runtime Capabilities
Detect Malware	Real-time detection and reporting of KNOWN and ZERO-DAY malware.
Remote Access:	<p>Ability to detect, report, and block the following in real-time.</p> <p>Legit Use of Remote Access</p> <ul style="list-style-type: none"> • <u>Screen Sharing Active</u> - Social Engineering - Scammer leverage Remote Access functionality like Zoom, Microsoft Teams, TeamViewer <p>Unauthorized Use of Remote Access</p> <ul style="list-style-type: none"> • <u>Sideloaded Risky Malware</u> - Malware with Remote Access (RAT) functionality, Trojan, Bot that are sideloaded <p>Risky Permission</p> <ul style="list-style-type: none"> • <u>Accessibility Active</u> - Sideloaded Apps that abuses Accessibility Permission
Sideloaded Apps with Accessibility Permission	<ul style="list-style-type: none"> • Real-time detection, reporting, and blocking of sideloaded apps with Accessibility permissions.
Screen Sharing/Mirroring:	<ul style="list-style-type: none"> • The ability to detect, report, and block Screen Sharing/Mirroring instances when the banking app is open.

ASEAN Regulations Follow Suit

In addition to MAS, regulatory bodies such as the Hong Kong Monetary Authority (HKMA), Malaysia's RMIT, and the Reserve Bank of India (RBI) are implementing similar regulations.



Hong Kong Monetary Authority

Enhanced Digital Banking Security



Malaysia

Risk Management in Technology (RMIT)



Reserve Bank of India (RBI)

Digital Payment Security Controls

Conclusion: Embrace Regulatory-Grade Security for Mobile Banking Apps

In today's rapidly evolving digital landscape, particularly in the mobile-first banking sector, Singaporean banks face the dual challenge of adhering to MAS guidelines and addressing ever-changing mobile app threats. Zimperium's adaptive security solutions offer a robust path forward, aligning with regulatory requirements while proactively safeguarding against emerging cyber threats. By integrating advanced security measures, Zimperium not only enhances the defenses of banking apps but also ensures user privacy protection, thereby maintaining trust in the financial ecosystem. With Zimperium's solutions, banks can fortify their mobile applications, making them not only smarter but also safer, thus meeting the imperative need for security in the dynamic digital banking environment.

To learn more, please [contact us](#).



Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244