Monetary Authority of Singapore
10 Shenton Way MAS Building Singapore 079117 Telephone: (65) 6225 5577 Facsimile: (65) 6229 9229

Circular No. MAS/TCRS/2023/01

05 April 2023

To Chief Executive Officers of All Financial Institutions

Dear Sir / Madam

CIRCULAR ON ADDRESSING RISKS THAT ARISE FROM THE THEFT AND MISUSE OF AN INDIVIDUAL'S PERSONAL INFORMATION

Background

Data breaches involving the loss or leakage of personal information held by organisations are often the result of cyber-attacks or the mis-handling of information. Criminals have been known to use leaked personal information to perpetrate fraudulent financial transactions by impersonating victims over non-face-to-face communication channels such as the internet or phone.

Security principles in identity verification

2. To guard against risks arising from impersonation attacks, financial institutions ("FIs") should adopt the security principles that are set out in the following when verifying an individual's identity:

a) Use at least one of the following types of information in the customer authentication process:
    i. Something that only the individual knows, such as a password or a personal identification number;
    ii. Something that only the individual has, such as a cryptographic identification device or token;
    iii. Something that uniquely identifies the individual, such as the individual's biometrics or behaviour; or
    iv. Information that is only known between the individual and the FI, such as account transaction information or application identification number.

b) Implement additional authentication[1] for high-risk activities including, but not limited to:

[1] Require customers to verify their identity using information that has not been used in the customer authentication process mentioned in paragraph 2a.

i. changes to sensitive customer data (e.g., customer address, email, phone number);
ii. registration of third-party payee;
iii. high value funds transfers; and
iv. revision of funds transfer limits.

3. FIs should assess identity theft and account takeover risks that stem from the use of stolen personal information and implement processes and controls to effectively mitigate these risks.

4. In the context of online financial services, Section 14 of the MAS Technology Risk Management Guidelines[2] expects FIs to implement real-time fraud monitoring systems to identify and block suspicious or fraudulent online transactions. This can include systems to monitor the use of geolocation data, device characteristics, timing of request patterns, browser metadata and systems that detect fraud modus operandi to identify potential fraud. FIs should also review suspicious login attempts and transactions promptly.

5. FIs are ultimately responsible and accountable for ensuring that an individual is who he or she claims to be before undertaking any transactions for the individual, or acting on instructions from the individual. FIs should ensure that the identity verification measures that they have adopted are commensurate with the risks posed by the theft and misuse of personal information.

TOMMY TAN
DIRECTOR & HEAD (DIVISION I)
TECHNOLOGY AND CYBER RISK SUPERVISION DEPARTMENT

[2] https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines