FINANCIAL SERVICES COMMISSION

INFORMATION CIRCULAR

REPORTING CYBER INCIDENTS

The Financial Services Commission (the Commission) issued its Technology and Cyber Risk Management Guideline in 2024, which outlines the obligations and expectations of financial institutions (FIs) with respect to managing their cyber and technology related risks.

FIs are required to notify the Commission of all reportable cyber incidents and also report unsuccessful attempts of any cyber incidents.

To aid FIs in fulfilling their obligations:

1. Instructions on completing cyber incident reporting forms have been provided in the document accompanying this circular and the reporting forms are located on the Commission's website and can be accessed via embedded links in the instruction manual.

2. Examples of reportable cyber incidents are noted in the table below for reference.

Examples of Reportable Incidents

Table 1 below provides some examples of the types of reportable incidents but should not be considered an exhaustive list.

Scenario Type	Scenario Description	Impact
BIN *(Bank Identification Number)* Attack	An act of guessing an accurate combination of a debit/credit card number, the associated card verification value (CVV), and the card expiration date using brute force computing.	1. Unauthorised transactions 2. Loss of funds 3. Reputational damage
Cyber Attack	An account takeover is targeting online services with the use of new methods. The FI's current defenses are failing to prevent its customers' accounts from being compromised.	1. High volume and velocity of attempts 2. Current controls are failing to block attacks 3. Customers are locked out 4. Indication that customer account(s) or information has been compromised
Service Availability & Recovery	Technology failure at data centre.	1. Critical online service is down, and alternate recovery option failed 2. Extended disruption to critical business systems and operations
Third-Party Breach	A material third party is breached, the FI is notified that the third party is investigating	1. Third party is designated as material to the FI 2. Impact to FI data is possible
Extortion Threat	The FI has received an extortion message threatening to perpetrate a cyber attack	1. Threat is credible 2. Probability of critical online service disruption

Table 1: Examples of Reportable Incidents