

Appendix I – Examples of Reportable Incidents

The following table provides some examples of the types of reportable incidents but should not be considered an exhaustive list.

Scenario Type	Scenario Description	Impact
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.	<ol style="list-style-type: none"> 1. High volume and velocity of attempts 2. Current controls are failing to block attack 3. Customers are locked out 4. Indication that customer account(s) or information has been compromised
Service Availability & Recovery	Technology failure at data center	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Threat is credible 2. Probability of critical online service disruption