OSFI Technology and Cyber Incident Report

1. Incident & Contact Information

Incident Name or Identifier:	
Date and Time Discovered/Detected:	**Date and Time Occurred**:
Name of your Institution:	
Key Contact's Name	Key Contact's Position
Key Contact's Email	Key Contact's Phone Number
Incident Lead's Name	Incident Lead's Position

2.Site Location and Lines of Business Affected

Name of Business Line or function Affected	
Technology Asset(s) Affected	
Site/Location Affected	

3. Description of Risk & Incident

Incident Category	Where did the incident occur?
☐ Technology ☐ Cyber ☐ Other (specify below)	☐ FRFI ☐ Third Party ☐ Supply Chain ☐ Other (specify below)
If other, please specify:	**If other, please specify:**

Provide the incident type(s):

☐ Technology asset* outage	☐ DDoS	☐ Ransomware
☐ Technology asset* degradation/delay	☐ Insider Threat	☐ Unauthorized Access
☐ ABM Jackpotting	☐ Malware - Other	☐ Loss/theft of equipment
☐ Account take-over	☐ Malware Campaign	☐ Other (specify below)
☐ Cyber Crime	☐ Online Extortion	
☐ Data breach/leak	☐ Phishing	

***A "technology asset" is something tangible (e.g., hardware, infrastructure) or intangible (e.g., software/application, data, information) that needs protection and supports the provision of technology services**

If other, please specify:

Select an incident level or priority from the drop-down list.	Select one:
If other, please specify:	

Provide additional details below including: current state, known direct and indirect impacts, actions completed and pending, with estimated timelines to address the remediation of the incident.
Add description of root cause, if known

Provide description of sensitive information compromised or at risk. If no sensitive information is at risk, please indicate N/A	
Provide details on the tactics, techniques and procedures involved in the incident.	Provide the indicators of compromise.

Internal and External Notifications	
Has senior management been notified?	Date and time senior management was notified (if applicable)
Select one:	
Have other regulators or supervisory agencies been notified?	Date and time regulatory or supervisory agencies were notified (if applicable)
Select one:	

Provide names of other notified regulatory or supervisory agencies.

Have any law enforcement authorities been notified?	Name of notified law enforcement authorities
Select one:	
Have any cyber insurance providers been notified?	Name of cyber insurance providers used
Select one:	
Has a cyber and/or an insurance policy claim been initiated?	Has an external forensics firm been engaged?
Select one:	Select one:
Has a breach coach been engaged?	Has internal or external legal counsel been engaged?
Select one:	Select one: