

February 5, 2025

**CIRCULAR LETTER TO ALL INSTITUTIONS:**

*LICENSED OR ISSUED A FINANCIAL HOLDING COMPANY PERMIT UNDER THE FINANCIAL  
INSTITUTIONS ACT, 2008*

*REGISTERED UNDER THE INSURANCE ACT, 2018*

*LICENSED UNDER THE EXCHANGE CONTROL ACT CHAP 79:50*

*PAYMENTS SYSTEM OPERATORS OR PAYMENT SERVICES PROVIDERS PURSUANT TO THE FIA OR CBA*

*E-MONEY ISSUERS REGISTERED UNDER THE E-MONEY ISSUER ORDER, 2020*

**REF: CB-OIFI-399/2025**

**MANDATORY CYBERSECURITY INCIDENT REPORTING**

Due to the increasing threats to cybersecurity and the critical importance of maintaining the integrity and trustworthiness of our financial systems, the Central Bank of Trinidad and Tobago (“Central Bank”) reminds all of its regulated financial institutions of the requirement to report any cybersecurity incidents within twenty-four (24) hours of becoming aware of them. This requirement pertains to incidents that are deemed reportable under our regulatory framework, as noted in the Central Bank’s Cybersecurity Best Practices Guideline (“Guideline”).

As outlined in *Appendix II* of the Central Bank’s Guideline, as well as Section C of the Central Bank’s “*Instructions for Completing the Cybersecurity Incident Form*” (“*Instructions*”), regulated financial institutions are required to report promptly any incidents to the Central Bank that may have one or more of the following characteristics of a **material** nature, as follows: -

1. Impact has potential consequences for other companies or the domestic financial system;
2. Impacts the company's systems affecting financial market settlement, confirmations or payments (e.g., Financial Market Infrastructure), or impact to payment services;
3. Impacts operations, infrastructure, data and/or systems, including but not limited to the confidentiality, integrity or availability of customer information;
4. Disrupts business systems and/or operations, including but not limited to utility or data centre outages or loss or degradation of connectivity;
5. Causes the disaster recovery teams or plans to be activated or a disaster declaration has been made by a third-party vendor that impacts the company;

6. Impacts a number of external customers and/or negative reputational impact is imminent (e.g., public and/or media disclosure);
7. An incident assessed by the company to be of high or critical severity or ranked Priority/Severity/Tier 1 or 2 based on the company's internal assessment; and
8. Incidents that breach internal risk appetite or thresholds as per the cybersecurity strategy or policy.

Examples of incidents that the Central Bank would typically expect financial institutions to report include, but are not limited to:

- a. **Cyberattacks** which disrupt the successful delivery of financial services such as:
  1. A large-scale distributed denial of service (“DDOS”) attack on a cloud service provider, or other critical third-party service provider; and
  2. Social engineering (via email, social media, phone call, text message, etc.) leading to unauthorised wire transfers or electronic card purchases, the theft of customer deposits, or the loss of sensitive corporate or customer data, compromising its confidentiality.
- b. **Process failures** and/or **System Update failures** which significantly disrupt the delivery of financial services, such as:
  1. Failed batch processing preventing mass salary or pension payments;
  2. Card payment processing delays affecting merchant transactions;
  3. Application or database upgrades that corrupt customer records or monthly statements; and
  4. Mobile app updates that cause user authentication issues or inadvertently expose customer data.
- c. **Infrastructure problems**, including extended power outages or infrastructure damage from extreme weather, such as:
  1. Flooding affecting backup power systems, leading to power failures at multiple locations; and
  2. Fibre optic cable damage adversely disrupting online services.

For incidents that do not align with or contain the specific criteria or examples listed above, or when a company is uncertain, notification to the Central Bank is encouraged. Institutions should therefore institute adequate policies, procedures and processes to identify and report a material cybersecurity incident in a timely manner.

The Central Bank has established the following timelines to ensure the prompt and structured handling of cybersecurity incidents:

Activity/Report	Submission Timeframe
Initial Notification	Within 24 hours of becoming aware of a cyber-incident
Complete Cyber Incident Reporting	Within 72 hours of the incident
Subsequent Reporting	Regular updates (e.g., daily) as new information becomes available  Ongoing situation updates until incident containment/resolution  Post-incident review and lessons learned report following incident closure

Note: Where specific details are unavailable at the time of the initial report, the institution must:

- Indicate "information not yet available";
- Provide best estimates and all other available details; and
- Include expectations of when additional information will be available

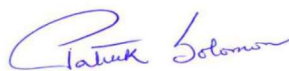
To ensure a streamlined reporting process, financial institutions should submit a Cybersecurity Incident Report Form to [cyberincident@central-bank.org.tt](mailto:cyberincident@central-bank.org.tt), sending a copy to their designated Relationship Officer.

The Guideline, the Cyber Incident Reporting Form, and the Instructions can be accessed on the Central Bank's website at <https://www.central-bank.org.tt/core-functions/supervision/cybersecurity>.

Please be guided accordingly and kindly acknowledge receipt of this letter electronically.

We look forward to your cooperation in ensuring the timely reporting of any material cybersecurity incidents.

Yours sincerely



Patrick Solomon  
**INSPECTOR OF FINANCIAL INSTITUTIONS**