# Cayman Monetary Regulatory Authority International

At the forefront of financial regulation, the Cayman Monetary Regulatory Authority International (CMRAI) is dedicated to upholding the highest standards of financial oversight and compliance. Our mission is to safeguard the stability and integrity of the global financial system by ensuring that financial services operate within a framework of transparency, accountability, and excellence.

As a trusted partner to financial institutions worldwide, CMRAI provides rigorous supervision, innovative solutions, and strategic guidance to foster a secure and thriving financial environment. With decades of experience and a commitment to global standards, we stand as a pillar of trust and security in an ever-evolving financial landscape.

With a legacy of excellence in financial oversight, the Cayman Monetary Regulatory Authority International (CMRAI) is a beacon of trust in the international financial community. Our role extends beyond regulation; we are innovators, collaborators, and protectors of the global financial ecosystem. By fostering compliance, promoting best practices, and embracing technological advancements, CMRAI ensures that financial services remain resilient and adaptable in a dynamic global market.

Our comprehensive approach to regulation encompasses a deep understanding of financial risks and a proactive stance on emerging challenges. We are committed to empowering financial institutions with the tools and guidance necessary to navigate complex regulatory landscapes, thereby contributing to global economic stability and growth.

Cayman Islands Monetary AuthorityReference No.XXXX Cyber Incident Report Instructions: 1. Notify the Authority promptly. For new incidents complete and submit the entire form. 2. Form to be completed by a member of staff authorised by the Board of Directors to discuss the incident. 3. Unless otherwise advised, weekly updates are required by the Authority until such time as the Authority is satisfied that the incident has been satisfactorily resolved. 4. Follow up reports to a specific incident, please complete relevant fields relating to update and reference previous incident report(s) in Section A (2). Section A. 1Filing Particulars Date and Time of notification to CMRAI [day/month/year ; time] Licensee/Registrant Name[insert text] Licences/Registrations Affected Licence and/or Registration Type (check all that apply) Licence/Registration Number [insert text] Name of Authorised staff member filing This Report [insert text] Position Held [insert text] Contact Details (telephone number and address) [insert text] 2Case Is this filing related to a previously reported incident?[Select from drop-down list] [if "Yes" selected, provide additional Reference Number of original incident] Type of Threat/Incident[Select from drop-down list] [if "Other" selected, provide additional details here] Event Description [insert text] Date and Time Incident Discovered01-Jan-2018 12:30PM Jurisdiction in which the incident was discovered: [insert text] Have other entities within the group structure been affected? [Select from drop-down list] [if "Yes" selected, provide additional details here] Who has been impacted by the incident? Who discovered the incident?[Select from drop-down list] [if "Other" selected, provide additional details here] Who has been notified of the incident? [Select from drop-down list] [Select from drop-down list] [Select from drop-down list] [if additional persons are notified please select "Other" and provide additional details here] How has this incident been classified?[Select from drop-down list] [Select from drop-down list] [Select from drop-down list] [if additional classifications are required please select "Other" and provide additional details here] Does the Licensee have a cybersecurity plan in place?[Select from drop-down list] Has the Licensee invoked its cybersecurity plan?[Select from drop-down list] (i) If no plan invoked, provide details of actions taken. [insert text] Has the Licensee engaged a third party to assist with the matter?[Select from drop-down list] (i) If so, provide third party details including qualifications and relevant experience in handling cyber security matters. [insert text] Is the incident contained?[Select from drop-down list] (i)If no, provide details of steps being taken to resolve the issue. [if "No" selected, provide additional details here] 3Assessment Resulting impact of incident Type (check all that apply) Is it evident whether the incident has resulted in the Licensee's breach of any relevant laws and/or regulations of jurisdictions in which it operates? [Select from drop-down list] [if "Yes" selected, provide additional details here] Does this incident span across other jurisdictions?[Select from drop-down list] Loss of Client Data Loss of Licensee/Non-Client Data Loss of confidential/sensitive information Bank Licence (Class A or Class B) Corporate Services Licence Companies Management Licence Controlled Subsidiary (Trust) Insurance Licence Mutual Fund Administrators Licence (Full or Restricted) Private Trust Company (PTC) SIBL Licence SIBL Excluded Person Trust Licence (Full / Restricted/ or Nominee) Group Entities (if applicable) Regulated Parents Unregulated Parent Regulated Subsidiaries Unregulated Subsidiaries Clients Sub -Contractors Business Associates Loss of Personally Identifiable Information Loss of Payment Card Information Loss of usernames or passwords Temporary loss of access to systems Permanent loss of access to systems Physical damage [if "Yes" selected, provide additional details here] Provide details of actions taken as at the filing of this report. [insert text] 4Analysis Has the root cause of the incident been determined?[Select from drop-down list] [if "Yes" selected, provide additional details here] Has the Licensee determined a solution to the problem?[Select from

drop-down list] [if "Yes" selected, provide additional details here] Have customers, clients, staff, been formally notified?[Select from drop-down list] [if "Yes" selected, provide additional details here] 5Remediation Has an incident management team been established?[Select from drop-down list] [if "Yes" selected, provide additional details of composition and roles/responsibilities here] Detail proposed remediation steps. [insert text] 6Technical details What is the source of the breach?[Select from drop-down list] [if "Other" selected, provide additional details here] If the source is external, do you know the IP address of servers/persons involved in the breach? [Select from drop-down list] [if "Yes" selected, provide details of IP addresses(s) here] Have any steps been taken to secure chain of custody of any evidence? [Select from drop-down list] [if "Yes" selected, provide additional details here] Have you preserved system log files?[Select from drop-down list] If "Yes" selected above, have system log files been subjected to a hash algorithm to ensure admissibility? [Select from drop-down list] [if "Yes" selected, provide additional details here] Was there any transactional data loss that cannot be recovered?[Select from drop-down list] [if "Yes" selected, provide additional details here]