5.4 Information Security

5.4.1 Information Security Management Policy

To enhance the quality and stability of financial services and effectively manage information security risks, CUB has established the Information Security Policy following the information security blueprint of its parent company, Cathay FHC. This policy serves as the guiding principle for implementing information security protection measures, continuously strengthening cybersecurity capabilities, and achieving secure, convenient, and uninterrupted financial services. The Bank has set up an Information Security Department as the dedicated unit responsible for formulating the bank-wide information security policy, planning the information security architecture blueprint, coordinating the handling of major information security incidents, reviewing information security defense mechanisms, and reviewing emergency response plan inspection. It supervises the overall implementation of information security, conducts information security advocacy and education training, and reviews compliance with information security laws and regulations. In 2022, the Bank established the position of Chief Information Security Officer to oversee the promotion of information security policies and the allocation of related resources. The Information Security Department submits an annual report on the overall implementation of information security to the Board of Directors and holds Information Security Committee Meetings supervised by the President and relevant department heads every half year.

The authority for approving the Information Security Policy is the Board of Directors, which annually reviews to ensure the confidentiality, integrity, availability, and legality of information assets. To ensure compliance with and promotion of information security policies, as well as to supervise and coordinate information security management efforts, CUB has established a cross-departmental "Information Security Committee." Chaired by the President, the committee includes supervisory heads from information-related, legal, regulatory compliance, risk management, information security, and digital transformation units. The Chief Information Security Officer serves as the executive secretary, and the committee convenes meetings at least every half year.

To adapt to industry trends, emerging technologies, and cloud applications, CUB adheres to relevant regulations and self-regulatory standards to maintain the validity of international cybersecurity certifications. This includes verification by third-party independent organizations for ISO 27001:2022 every half year, as well as annual verification for Payment Card Industry Data Security Standard (PCI DSS). Additionally, CUB has implemented the "Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT)" and the "National Information Security Center's Government Agency Information Security Governance Maturity Assessment Mechanism" to assess cybersecurity maturity. Based on assessment results, regular reviews and improvements are undertaken. Annually, independent professional consultants are engaged to conduct information security assessments, ethical hacker hacking tests, and implement necessary enhancements to continuously strengthen the Bank's information security defenses. Furthermore, recognizing the evolving nature of financial service outsourcing and cross-industry collaborations, CUB reinforces its third-party information supplier management mechanisms to avoid potential information security risks originating from the supply chain.

5.4.2 Information Security Action Plan and Achievements

- **Collaborated with third-party professional consultants to assess the implementation of information security both domestically and internationally:**

In order to enhance overall information security and comply with regulatory requirements in the financial industry, the Bank conducts regular computer system security assessments including our overseas branches every year. An independent professional consulting firm is engaged to evaluate the Bank's overall information security performance annually. The assessment results, along with an internal control statement, are submitted to the Board of Directors before the first quarter of the following year. Additionally, to gain deeper insights into the information security practices at overseas branches, information security personnel, along with third-party consultants, conduct on-site inspections. This ensures that operations at overseas branches comply with information security regulations and adhere to various security control requirements, aiming to embed information security into the corporate culture and enhance the Bank's overall security posture.

- **Implementing financial cybersecurity action plans:**

The Bank has completed the items under the "Financial Cyber Security Action Plan 1.0" issued by the Financial Supervisory Commission, including the appointment of a Chief Information Security Officer, establishment of an Information Security Advisory Group, adoption of international cybersecurity and business continuity management standards with verification, alignment with the Group's computer security incident response plan, conducting cybersecurity governance maturity assessments, establishing a cybersecurity monitoring service center mechanism,

encouraging cybersecurity personnel to obtain international certifications, and incorporating practical business operations verification into offsite backup drills. In response to the "Financial Cyber Security Action Plan 2.0" released on December 27, 2022, the Bank has completed additional initiatives such as completing Breach and Attack Simulation (BAS), initiating the implementation of a zero trust framework, and implementing a project for safeguarding data in response to major cybersecurity incidents and natural disasters. These efforts aim to continuously strengthen the Bank's cybersecurity capabilities, ensuring the provision of secure, convenient, and uninterrupted financial services, and enhancing the Bank's information security management.

- **Information Security Protection and Strengthening Measures:**

The Bank regularly conducts computer system information security assessments, various contingency drills, penetration testing, cloud service safety configuration testing, intrusion and attack simulation drills, and white hat hacker red team drills, as well as strengthening measures for customer service program testing. Additionally, we implemented mechanisms for information security intelligence collection and processing, a security monitoring center, and incident response mechanisms to be well prepared at all stages for various emerging cybersecurity threats. Furthermore, the Bank annually invests in cybersecurity insurance to ensure appropriate measures are in place against all new types of cybersecurity threat, protect its and its customers' interests, and minimize losses from cybersecurity incidents. This year, a total of 205.3 million was spent for cybersecurity expenses, including software and hardware licenses, personnel training, etc., accounting for 1,098.67 million, which is approximately 18.6% of the Bank's total information budget. The Bank also encourages employees to obtain cybersecurity certifications, with a total of 164 cybersecurity certifications achieved by the end of this year, covering both management and technical certifications such as ISC2 CISSP/CC, ISACA CISM/CISA/CRISC, ISO 27001/27017/27018/27701/42001, EC-Council CEH/ECSA/CHFI/ECIH/CTIA, CompTIA Security+, iPAS Mid-level Cybersecurity Engineer, and other certification.

5.4.3 Defensive measures for transaction systems and internal operations

CUB's security protection setup includes monitoring and defense against abnormal network traffic, network firewalls, web application firewalls, intrusion detection and prevention systems, as well as endpoint protection mechanisms (anti-virus and EDR). An Information Security Monitoring and Management Platform is established to aggregate security event logs from various security protection devices, and to centrally manage, store, search, and forward them to the Security Operation Center (SOC). This monitoring center provides 7×24 service and is responsible for analyzing and monitoring any messages that may violate the confidentiality, integrity, or availability of information in the system. Once abnormal events are detected, they are immediately reported, processed, and tracked to ensure the security of transactions and the effectiveness of protection measures.

5.5 Compliance

The Bank has established a Compliance Department to establish and execute mechanisms for disseminating legal updates, providing training, maintaining contact with legal compliance operations domestically and internationally, and promptly notifying the Board of Directors of any changes, ensuring that all operations comply with legal regulations. The Chief Compliance Officer regularly reports to the President on the implementation of the Bank's legal compliance system and reviews the content. Additionally, at least every half year, reports on the execution of legal compliance operations and the implementation of fair customer treatment principles are submitted to the Board of Directors and the Audit Committee. In the event of significant violations of laws or a downgrade by financial regulators, the Directors should be promptly notified, and matters of legal compliance should be reported to the Board and the Audit Committee to effectively supervise and promote the implementation of legal compliance operations throughout the Bank. In order to comply with regulatory supervision and the recommendations of financial inspections, the Compliance Department continues to plan optimization measures and responses for various legal compliance operations. The Compliance Department also provides opinions on new products, services, or business lines that whether it complies with regulatory requirements of regulatory authorities and internal policies. Through existing channels such as business contact meetings, training, supervisory management, and improvement review, the Bank will continue to supervise the implementation effectiveness of legal compliance affairs in domestic units and overseas branches. The Department will also thoroughly review and improve based on the opinions of regulatory authorities, the Cathay FHC, and the Bank's Internal Audit Department, aiming to achieve the goal of full compliance with laws and regulations. The Bank will introduce financial technology to optimize operational processes and establish a compliance system to centrally manage the execution of various legal compliance operations. Additionally, utilizing artificial intelligence (AI) technology to develop tools for analyzing the correlation between internal and external regulations.