Contents

About this Report

01 Sustainability Strategy Blueprint

02 Climate

03 Health

3.1 Health Promotion

3.2 Financial Health

04 Empowerment Strategy

05 Sustainable Finance

06 Sustainable Governance and Risk Management

07 Appendix

3.2.1 Anti-Fraud Guard Network

As a Domestic Systemically Important Bank (D-SIB), the Bank has taken on the responsibility of building a fraud-prevention protection network. Through online monitoring of new forms of criminal behavior, strengthened cash-flow management, enhanced information-security protection capabilities, and the integration of offline customer-service resources, we have built all-round anti-fraud strategies and technologies to safeguard the security of everyday financial transactions. We go further by actively improving the public's awareness of fraud so as to reinforce the first line of defense against scams.

Under the leadership of the President, the Bank has established a cross-departmental Anti-Fraud Taskforce that brings together expertise from different departments to build a sound anti-fraud governance structure. With an integrated anti-fraud mindset, the Bank has mapped out an anti-fraud blueprint, formulated comprehensive anti-fraud strategies and management objectives, and, by leveraging the "Cathay Shield"—which integrates data technology and staff empowerment—has established a joint defense mechanism spanning the four pillars of Knowledge Shield, Technology Shield, Care Shield, and Alliance Shield. This mechanism strengthens the Bank's ability to identify and intercept fraud. The Anti-Fraud Taskforce regularly reports progress to the Anti-Money Laundering and Countering the Financing of Terrorism Committee and the Treating Customers Fairly Committee to evaluate anti-fraud effectiveness and continuously refine anti-fraud strategies.

To encourage all units to proactively block fraud, the Bank has established special reward programs for the successful interception of fraud cases in addition to its existing reward rules. Employees who successfully block fraud are regularly recognized. In 2025, employees received a total of 8,793 recognitions for their successful fraud prevention efforts.

According to statistics from the National Police Agency of the Ministry of the Interior, the Bank ranked among the industry's top performers in the total amount of fraud successfully blocked at the counter in 2025. Through practical action, the Bank protects customers from financial losses, gradually builds a comprehensive omni-channel anti-fraud awareness strategy tailored to audiences of different ages, and enhances vigilance against fraud across society. The Bank also continues to introduce protection mechanisms from the perspective of victims, laying a foundation for further strengthening account security and customer protection mechanisms.

Looking ahead to 2026, the Bank will further strengthen anti-fraud measures and is committed to building a comprehensive anti-fraud ecosystem. This includes achieving cross-institutional joint anti-fraud capability through exchanges of experience and resource sharing among financial institutions, thereby accelerating identification of and responses to fraud patterns, as well as cooperating with the public sector to strengthen data-capture effectiveness based on actual fraud cases. Through such cooperation, the Bank will not only enhance its ability to identify potential criminal cases but also create a safer financial environment for customers.

In addition, the Bank continues to pay close attention to the potential of AI as a tool to support risk-control manpower and improve efficiency. Going forward, the Bank will continue to deepen the digital security network together with customers, industry peers, and regulators, becoming a fortress that safeguards assets and a trusted digital-finance partner for customers.

2025 Performance

Online Platform

- Effectively handled and removed 11 counterfeit websites and social media accounts.

Credit Card Transactions

- Successfully blocked abnormal transactions totaling NT$677 million.
- Blocked 3,241 suspicious cards.
- Successfully intercepted 45,927 unauthorized transactions.
- The early-warning detection rate was on average approximately 38% higher than that of peers.

Deposit & Remittance

- Successfully intercepted 4,374 fraud cases at the counter, with a cumulative blocked amount of NT$3.124 billion.
- Set abnormal-control rules for 45,435 accounts and blocked abnormal cash flows totaling NT$4.748 billion.

Educational Campaigns

- Cumulative anti-fraud education and outreach exceeded 69.9 million person-times for the year.

Note: The 2025 performance data is based on the Bank's internal statistics as of December 31, 2025.

Contents

About this Report

01 Sustainability Strategy Blueprint

02 Climate

03 Health

3.1 Health Promotion

3.2 Financial Health

04 Empowerment Strategy

05 Sustainable Finance

06 Sustainable Governance and Risk Management

07 Appendix

Cathay Shield

Four-pronged Joint Defense Mechanism

Knowledge Shield

- In 2025, the Bank extended fraud awareness education to younger audiences by signing a tripartite memorandum of understanding (MOU) with the National Police Agency of the Ministry of the Interior and the K-12 Education Administration of the Ministry of Education. Together, the parties launched the "Report Online, Call 165, Speak Up" anti-fraud program for schoolchildren, developing age-appropriate anti-fraud teaching materials for elementary school teachers nationwide. The program aims to strengthen children's understanding of the rule of law and self-protection skills, thereby reducing the risk of fraud targeting children and youth. More than 100 anti-fraud awareness sessions were delivered on campuses throughout the year.
- The Bank also partnered with the iconic Taiwanese snack brand Kuai Kuai to launch the limited-edition "Cathay United Bank X Kuai Kuai Anti-fraud Co-branded Pack." Featuring a blank face design on the packaging for consumers to draw on creatively, the campaign served as a reminder that fraudsters may appear in many different guises and encouraged the public to remain cautious when encountering unfamiliar information. In addition, the Bank launched the online "Anti-fraud Readiness" quiz. Through both online and offline outreach, as well as engaging and educational activities, the initiative helped reinforce anti-fraud awareness and improve the public's ability to recognize fraud.
- The Bank released four short videos under its "Technology for Security Protection" series, which accumulated more than 1.7 million views.
- Through its owned media channels, including EDM, Facebook, and LINE, the Bank shared information on fraud schemes and anti-fraud awareness, reaching more than 25 million impressions.
- In 2025, the Bank held a total of 418 anti-fraud awareness events, including 10 online events, with total participation exceeding 79,000.

Technology Shield

- Established monitoring rules based on common suspicious or clearly abnormal transaction patterns published by the Bankers Association, and issued alerts through system controls and abnormal account detection reports.
- Strengthened the identification of impersonation and fraud risks in application cases through the fraud detection system.
- Continued to monitor suspicious credit card transactions in real time through the early warning detection system and a 24-hour professional team, activating investigation and interception mechanisms. When impersonation fraud is suspected, the Bank proactively suspends credit card transactions and blocks abnormal merchants to prevent fraudulent card use.
- Leveraged technology to prevent and detect fraudulent activities.

Precautions Beforehand

- ✓ Procured internationally recognized real-time detection and takedown services for fraudulent impersonation websites. In 2025, the Bank also developed its own AI-Powered Online Bank Impersonation Detection System, combining automated web crawling with image and text recognition technologies to expand detection coverage and enhance monitoring effectiveness.
- ✓ Regularly collected dark web intelligence and, upon identifying any leakage of customer information, immediately implemented corresponding protective measures. The Bank also introduced digital signatures for emails sent to customers to ensure that email content has not been spoofed or tampered with.
- ✓ Partnered with Cathay Century Insurance to launch "Account Security Insurance." CUBE App users who complete the security settings required under the "Account Security Checkup" can enjoy enhanced protection and become eligible to participate in the "Account Security Insurance" program, making their digital financial experience more secure and reassuring.
- ✓ The CUBE App's "Card Security Lock" feature allows customers to flexibly set transaction time, location, type, and single-transaction amount limits according to their needs, effectively protecting the security of credit card and debit card transactions. The "SMS Inbox" feature helps customers verify messages in real time and quickly identify official SMS messages sent by the Bank.
- ✓ Introduced the FIDO2 biometric authentication mechanism into the online card payment verification process. By leveraging public-private key encryption, biometric recognition, and the Client to Authenticator Protocol (CTAP), the Bank enhances transaction security and helps prevent fraudulent card use through phishing and remote device manipulation.
- ✓ Enhanced the security of in-app Apple Pay card provisioning in the CUBE App by requiring credit cardholders to complete "device binding" through mobile phone number verification or ATM verification before proceeding with card linking, thereby preventing unauthorized enrollment of their cards into mobile payment services.
- ✓ Strengthened protection mechanisms for card linking within merchant apps by introducing mobile phone number verification and real-time card-linking alerts to ensure that the cardholder is the person performing the action.

Responses Afterwards

- ✓ Conducted daily real-time analysis of transaction patterns in fraud and unauthorized card use cases, and continuously refined and optimized detection rules to improve the accuracy of the early warning detection system.
- ✓ Continuously adjusted detection rules within the 3DS verification system, monitored abnormal transactions in real time on a daily basis, and blacklisted merchants and device IP addresses involved in fraudulent activity to block online verified transactions.
- ✓ Introduced Cathay Shield's real-time risk detection mechanism to accurately monitor abnormal fund flows and shorten the time gap between suspicious account activity and the Bank's account restriction measures.
- ✓ Built an "Abnormal Fund Flow Exploration Platform" that combines big data and visualization modules to lower technical barriers, enabling anti-fraud analysts without engineering backgrounds to quickly perform pattern modeling and rule testing. This accelerates the adjustment and deployment of risk control strategies and strengthens the defense system's ability to evolve continuously.
- ✓ Applied breakthrough federated learning technology through the "Finshield" project, enabling financial institutions to collaboratively train technology-based anti-fraud models without exchanging personal data. This helps identify new fraud patterns, expand detection coverage, and effectively address the data silo challenges faced by financial institutions.

Contents

About this Report

01 Sustainability Strategy Blueprint

02 Climate

03 Health

3.1 Health Promotion

3.2 Financial Health

04 Empowerment Strategy

05 Sustainable Finance

06 Sustainable Governance and Risk Management

07 Appendix

Cathay Shield
Four-pronged Joint Defense Mechanism

Care Shield

- All employees are required to complete anti-fraud awareness training.

"Fraud Identification and Prevention Workshop" training program

- ✓ Enhances employees' professional knowledge and anti-fraud awareness in handling abnormal situations at branch counters across all 165 branches.
- ✓ Covers the Bank's key control procedures and tools, fraud scenario analysis, techniques for asking follow-up questions with care and vigilance, as well as case studies and drills.

Branch Operations Management Monthly Meeting

- ✓ Provides reminders on key follow-up questions based on the analysis of warning patterns and fraud scenarios.
- ✓ Reviews and analyzes fraud cases in which interception at the counter was unsuccessful, with the aim of strengthening the depth of customer follow-up and inquiry.

Communication guidelines for high-risk businesses / transactions

- ✓ Developed the "KYC Communication Guide for High-risk Business Services" and the "High-risk Transaction Counter Communication Guide" to provide practical inquiry techniques for different scenarios.

Fraud alerts and anti-fraud cases sharing

- ✓ Regularly issues the latest fraud alerts and shares exemplary fraud prevention cases for reference.

- Each branch has designated anti-fraud champions and established an internal reporting group, "C_Team Anti-fraud Vanguard." When branch staff identify unusual circumstances during customer applications or over-the-counter transactions, such as suspected victimization or fraud, they may, depending on the situation, contact the customer's family members or local police officers to provide assistance. Anti-fraud champions are required to report over-the-counter interception cases in the group, enabling the real-time sharing of case information and handling approaches across branches, promoting cross-branch communication and collaboration, and strengthening the Bank's overall anti-fraud response capabilities.
- The operating guidelines for deposit and remittance services require strict implementation of identity verification and customer due inquiry. Account opening procedures must be completed in accordance with the checklist, item by item. When handling applications for automated service items, staff must understand the purpose and reasonableness of the customer's transactions, conduct enhanced KYC checks based on the checklist, and record the results. Relevant review items have also been incorporated into internal self-inspection procedures to highlight key control points and assess the effectiveness of implementation.
- The Bank established a user risk rating detection module and prioritized its application in the review process for high-risk business applications. Enhanced customer due inquiry is conducted for medium- and high-risk users.
- The Bank has established relevant handling procedures for accounts suspected of being used by someone other than the account holder and implemented corresponding control measures.

Alliance Shield

- Collaborated with Cathay Financial Holdings (Cathay FHC), the Ministry of Justice Investigation Bureau, the Criminal Investigation Bureau, the Taiwan High Prosecutors Office, and local district prosecutors offices to share anti-fraud intelligence.
- In 2025, the Bank signed memorandums of understanding on a suspicious financial accounts analysis project with three district prosecutors offices-Taipei, Ciaotou, and Shilin-establishing a real-time notification mechanism for suspicious financial accounts to strengthen fund flow monitoring and risk alerts.
- Partnered with the National Police Agency of the Ministry of the Interior and the K-12 Education Administration of the Ministry of Education to sign a tripartite memorandum of understanding (MOU) and jointly launch the "Report Online, Call 165, Speak Up" anti-fraud program for schoolchildren.
- Participated in anti-fraud forums organized by the Criminal Investigation Bureau and local police departments to exchange views on identifying fraud schemes and suspicious fund flows, thereby jointly enhancing anti-fraud capabilities.
- In 2025, branches reported more than 4,500 cases in which local police officers were contacted to provide on-site assistance after customers were suspected of being defrauded or involved in fraud.
- For suspected credit card fraud cases, designated investigators promptly compiled information on abnormal accounts, transaction trails, and related evidence, and worked with peer institutions to gather similar cases and swiftly report them to police authorities for analysis and investigation. This helped disrupt fraud chains at an early stage and prevent cases from escalating. A total of 162 such cases were recorded in 2025.