3.2 Financial Health

According to the definition of the United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA), financial health includes four elements: daily income and expenditure, financial planning, financial risk resistance and financial confidence. Through offering a diverse range of financial products and services, CUB aligns with the four elements of financial health and practices the value of financial inclusion. Our goal is to become "The Best Guardian of Customer Wealth" and "The Benchmark Enterprise for Financial Inclusion in Taiwan." This is achieved through the following four key areas:

1. **Anti-Fraud Guard:** To promote anti-fraud measures and raise awareness to help customers mitigate the impact of fraudulent activities;
2. **Digital Transformation and Innovation:** To drive digital transformation and develop innovative products, enabling customers to enjoy convenient one-stop digital financial services. We offer user-friendly financial planning tools that help customers make healthy financial decisions, effectively manage their finances, and utilize trusts to safeguard their assets;
3. **Financial Inclusion:** To enhance the resilience against financial risks and the accessibility of using online digital services for diverse groups such as small and micro businesses, SMEs, and social enterprises, while expanding their use of financial services;
4. **Financial Education:** Promoting financial education to raise public financial awareness, helping people make more reasonable financial decisions. This boosts their financial resilience and confidence, supporting individuals in building a confident and happy life.

Through these services, CUB hopes to enhance the financial health of our customers and build a solid foundation for a secure society.

3.2.1 Anti-Fraud Guard Network

As a D-SIBs, we shoulder the responsibility of building an anti-fraud guard network and safeguard the security of daily financial transactions through comprehensive anti-fraud strategies and technologies such as online monitoring of new criminal activities, management of cash flow, improvement of information security, and integration of offline customer services. Furthermore, we proactively enhance public awareness of fraud, reinforcing the first line of defense against fraudulent activities.

Under the leadership of the President, CUB has established a cross-departmental Anti-Fraud Taskforce in July 2023, bringing together expertise from various departments to create a comprehensive anti-fraud governance structure. With an integrative anti-fraud mindset, the Taskforce designed a blueprint for fraud prevention, formulated comprehensive strategies and management goals, and leveraged integrated data technology and staff empowerment through the "Cathay Shield." This framework incorporates four key components - "Knowledge Shield, Technology Shield, Care Shield, and Alliance Shield"- to establish a collaborative defense mechanism that strengthens fraud detection and prevention capabilities, creating a protective network to combat fraud. This Taskforce regularly reports its achievements to the Anti-Money Laundering and Counter Financing Terrorism Committee and the Treating Customers Fairly Committee, evaluates the effectiveness of anti-fraud measures, and continuously refines anti-fraud strategies.

Additionally, to encourage active fraud prevention across business units, the Bank has established a rewards program to commend employees who successfully prevent acts of fraud. The program was established in addition to original incentives. In 2024, a number of 7,817 awards won by employees for their successful fraud prevention efforts.

According to statistics from the National Police Agency of the Ministry of the Interior, in 2024, CUB topped the industry in terms of successfully preventing fraudulent transactions amount at bank counters. Through proactive actions, the Bank protects customers from financial losses, exerts a positive influence, enhances the community's awareness, and demonstrates an unwavering commitment to financial security, strengthening CUB's leadership position in anti-fraud efforts. Looking ahead to 2025, CUB will further enhance fraud prevention measures and work toward establishing a comprehensive anti-fraud ecosystem within the financial sector. Through experience exchange and resource sharing among financial institutions, CUB aims to implement cross-institutional fraud prevention, accelerating the identification and response to new fraud patterns. This will not only improve our ability to detect potential criminal activities but also create a safer financial environment for customers.

Category	2024 Results
Online Platforms	• Effective takedown of 27 counterfeit websites and social media accounts
Credit Card Transactions	• The interception of NT$ 996 million worth of abnormal transactions • The blocking of 2,396 instances of suspicious credit card bindings • Successful interception of 81,784 fraudulent card transactions • Early detection rate was on average 37% higher than the industry, with an annual growth rate of 14%
Deposit & Remittance	• Successful interception of 4,528 fraudulent cases at bank counters, with a number of 7,817 awards won by employees for their efforts. The total blocked amount reached NT$ 3.04 billion • Initiated controls over 57,865 accounts for abnormal transactions, blocking NT$ 1.58 billion in abnormal cash flows
Educational Campaigns	• Over 65 million exposures from fraud prevention education and promotional activities throughout the year

Note 2024 Results is derived from internal statistics as of December 31 of the same year.

Knowledge Shield

- In 2024, CUB published the first "Anti-Fraud Behavior Survey Report," revealing that everyone, instead of specific populations, are susceptible to frauds and that half of all fraud victims never report the incident. Therefore, we are in collaboration with the Criminal Investigation Bureau of the National Police Agency, launching the "Report online, Call 165, Speak up " initiative, and leveraged TV channels, social media, and on-site promotions to expose various fraud techniques and teach fraud detection skills. We expect to adopt various media across all age groups to improve their the ability to identify fraud.
- Launched 4 short videos on security technology protection, which garnered over 1.34 million views.
- Conducted a quiz-based anti-fraud campaign using MBTI personality tests to demonstrate the connections between fraud scenarios (investment fraud, romance scams, fake police scams, lottery scams, etc.) and personality traits. The campaign reached around 22.4 million exposures, with more than 18,000 online participants.
- For rural students, CUB's online financial education courses were designed to include fraud awareness, teaching children how to handle possible fraud situations targeting students.
- In 2024, 243 anti-fraud events (including 9 online) were held, with over 13,000 participants.
- Fraud techniques and detection were shared over self-media platforms regularly (including EDM, Facebook, LINE, ATM, etc.), reaching over 48 million impressions.

Technology Shield

- Based on common fraudulent or suspicious transaction patterns published by the Bankers Association, monitoring rules were established to provide system controls and alert reports for abnormal accounts.
- Leveraged a fraud detection system to strengthen identification of fraud risks associated with applications.
- Continued to monitor suspicious credit card transactions in real-time through the early warning detection system and a 24-hour professional team, triggering investigation and blocking mechanisms. If fraud is suspected, credit card transactions are temporarily suspended, and abnormal merchants are locked to prevent card skimming.
- Using Technology to Prevent and Detect Fraud.

Precautions Beforehand

- By purchasing the internationally renowned counterfeit and fraudulent website detection and removal service (RSA FraudAction Service). Once counterfeiting is discovered, the removal process will be immediately initiated, effectively stopping fraudulent activities from happening.
- By gathering intelligence from the dark web, we can promptly identify and address potential leaks of customer information (such as credit card numbers or account information) and take corresponding measures to protect customers from further losses.
- CUB has introduced digital signature authentication to verify the authenticity of email sources for recipients. This measure strengthens defenses against social engineering fraud techniques (such as ransomware or phishing emails).
- Provided a "Card Security Lock" feature for customers to lock their credit cards by region (domestic/overseas), type (physical/cardless), time, and amount, to safeguard credit card security.
- Improved device security for card binding, requiring TWID (by TWCA) SIM verification before allowing credit card binding to devices, preventing fraudulent card binding to mobile payment applications for cardholders.
- Strengthened the virtual card number (VCN) application by adding identity verification steps in the online application process to enhance verification strength and security. This reduces the risk of personal data fraud and counterfeit applications for VCN, mitigating the associated risk of fraudulent card use.
- Offered the "SMS Inbox" feature to allow customers to verify the source of SMS messages. When customers receive suspicious scam messages, they can log into their CUBE App to check the message instead of calling our customer service center to confirm the legitimacy of these messages.

Responses Afterwards

- Analyzed transaction patterns of fraud and fraudulent credit card use in real-time every day, continuously adjusting and optimizing detection rules to improve the accuracy of our early warning detection system.
- The 3DS verification system continuously adjusts detection rules, monitors abnormal transactions in real-time every day, and blacklists stores and device IPs used for fraud to block transactions requiring online verification.
- Leveraged the Cathay Shield risk detection platform to accurately monitor abnormal cash flows, implement real-time detection technologies, and accelerate the time from abnormal activities to initiation of lockdown controls.
- Partnered with other financial institutions to launch the "Cross-Financial Federated Learning Anti-Fraud PoC" through FinTech Space, a financial technology innovation hub, integrating model parameters from different organizations and successfully increasing abnormal account detection rates by 20%.
- A cross-departmental emergency response team was established to cooperate with domestic information security experts to share fraud techniques and prevention strategies and provide professional emergency response support.

Cathay Shield
Four-pronged Joint Defense Mechanism

Care Shield

- CUB requires all staff members to undergo "Fraud Recognition and Prevention Education", which includes (1) Through "Fraud Recognition and Prevention Workshops," training courses have been conducted to enhance the professional competence and anti-fraud awareness of employees in all 165 branches nationwide. The course covers key control points and tools used within the Bank, fraud scenario analysis, techniques for strengthening careful questioning, case studies, and hands-on exercises. (2) Through conducting pattern analysis of suspicious accounts and discussing scenarios of fraudulent techniques during monthly branch operational meetings offer key reminders. (3) Manuals such as "Service Desk High-Risk Transaction KYC Communication Handbook" and "High-Risk Transaction Counter Communication Skills" are compiled to provide various practical questioning techniques. (4) Regular fraud prevention reports are issued to disseminate the latest fraud information from the Criminal Investigation Bureau, share exemplary cases of fraud prevention, and provide updates on the latest anti-fraud information. (5) For failed fraud interception cases at the counter, analysis and review are conducted, and explanations and reminders are provided during monthly branch operational meetings, strengthening the depth of customer questioning through inter-bank case analysis and feedback.
- Each branch has designated "Fraud Prevention Seeds" and established an internal notification group called the "C_Team Anti-Fraud Vanguard". When a branch teller identifies suspicious behavior or potential fraud during customer applications or in-person transactions, the teller may contact the customer's family or local police to provide assistance as needed. These seeds can report on cases of attempted fraud or fraudulent activities intercepted at the counter. This facilitates simultaneous awareness among branches regarding interception situations and handling methods, reduces communication barriers, promotes mutual learning, and strengthens collaborative capabilities of the branches.
- CUB specifies in its "Deposit and Remittance Operations Principle" that "identity verification" and "caring questioning" must be implemented, and account opening procedures should be confirmed step-by-step according to the KYC checklist. For automated services, we must understand the purpose and reasonableness of the customer's transaction and strengthen the KYC checklist and recordkeeping. The requirement for enhanced questioning of customers and internally establishes relevant audit items to remind staff of the focus areas, reviewing implementation status.
- Developed a user risk rating detection module, which is prioritized in the review process for high-risk application services, with a focus on strengthening careful questioning for medium/high-risk users.
- Established relevant procedures to initiate corresponding control measures for any accounts suspected to be operated by someone other than the account owner.

Alliance Shield

- Join the "AI Intelligent Anti-fraud Alliance" and collaborating with Cathay FHC, the Ministry of Justice Investigation Bureau, the Criminal Investigation Bureau and the District Prosecutors Office to share fraud intelligence.
- Collaborates with the Criminal Investigation Bureau of the National Police Agency to stay updated on the latest fraud patterns and jointly promote the "Report online, Call 165, Speak up" campaign.
- Participated in anti-fraud seminars organized by the Central Police University, Criminal Investigation Bureau, and local police stations, exchanging insights on identifying fraud tactics and suspicious cash flows, and collectively improving fraud prevention expertise.
- Branches identified over 4,200 cases in 2024 where customers were suspected of being victims or perpetrators of fraud, leading to the involvement of local police officers for assistance.
- To prevent fraudulent activities as an organized crime, CUB provided detailed information about suspected credit card fraud cases to the police to expedite investigations. In 2024, a total of 67 such cases were reported.