As a bank, we commit in our social responsibility to guarantee clean financial flow and positive social impacts, we'd like to share a best practice of PPP in counter-fraud and also propose our comments as follows.

Section 1：Best Practice

Best Practice of PPP(Public-Private Partnership) in combating digital fraud in Taiwan：Eagle Eye Alliance

Vision and Mission:

As we all believe, financial institutions bear the mission and responsibility for "financial security" since they operate as chartered industries that raise public funds for utilization. With a development based on "integrity," they aim to become trustworthy and responsible. As technology and economic development changes, financial crimes such as internal corruption, external digital fraud, and money laundering become more frequent, leading to a shift in expectations for the financial industry's role. In Taiwan, the financial institutions now focus on responding to stakeholders' best interests, with "shared societal well-being" instead of maximizing shareholders' interest as the ultimate value. This perspective aligns with the growing importance of Environmental, Social, and Governance (ESG) principles, emphasizing the need for financial institutions to address not only economic performance but also their impact on society and the environment. In Taiwan, in total 34 banks established an Eagle Eye Alliance to display this vision and commitment.

Origin:

The origin of Eagle Eye Alliance comes from one of the bank(Taipei Fubon Bank) in Taiwan, started Project Eagle Eye. Project Eagle Eye is a groundbreaking digital fraud detection and prevention machine learning AI model, implemented on July 4th, 2022. Developed as the first artificial intelligence machine learning model in Taiwan specifically designed to address digital fraudulent activities as well as the first collaboration between law enforcement and financial institution, its primary goal is to ensure financial safety for customers. The model offers a comprehensive approach to digital fraud prevention, integrating early warning provisions across diverse communication channels such as physical branches, internet/mobile banking, and ATMs. Its real-time hotspot detection feature enables immediate

notification of the police network to apprehend money mules and mitigate potential financial losses.

Milestones of Project Eagle Eye

During the **development stage**, Taipei Fubon Bank collect data from the National Central Police Agency, using confirmed digital fraud transactions as a basis for comparison with normal transactions randomly sampled from our database. Feature engineering is employed to extract useful indicators that signal unusual behavior. Taipei Fubon Bank track the movement of money in and out of the bank using "Flow" and analyze activity logs on mobile/internet banking. The model is based on three subsets of information: transaction-related, behavior, and account. Taipei Fubon Bank construct a gradient-boosted decision tree to utilize all these features to determine the probability of an account being digital fraudulent.

In the **implementation period**, Taipei Fubon Bank apply gradient boosting to improve a single model by combining it with other models to generate a collectively strong model. Gradient boosting sets targeted outcomes for the next model in an effort to minimize errors, iteratively training an ensemble of shallow decision trees. The final prediction is a sum of all the tree predictions, minimizing bias and under fitting. Taipei Fubon Bank optimize the parameters by conducting a random search to test and find the combination that increases the accuracy of the model.

Benefits:

The impetus behind Project Eagle Eye was driven by the sharp increase in digital fraudulent activities during the COVID-19 pandemic, as scammers increasingly targeted online platforms. The traditional rule-based approach generated approximately 57,000 monthly alerts for Taipei Fubon, making effective inspection and response challenging. With the introduction of the machine learning model, false positives have been significantly reduced, and performance has improved over time. The model has achieved a 57.2% true positive rate and a remarkable 98% reduction in false positives, fortifying Taipei Fubon's ability to prevent digital fraud. Since implementing the model nine months ago, Taipei Fubon Bank have successfully halted an estimated TWD $193 million in fund flows. Consequently, financial safety for its customers is enhanced, and the bank's impact on society becomes increasingly positive._

The Eagle Eye Model has won 7 international financial innovation awards and 4 domestic awards to date.

Deterrence Efficacy Figure 1. Number of Accounts Flagged by National Police Agency

	Taipei Fubon Bank	Whole Banking Sector	Taipei Fubon's share of flagged accounts
2021 Total	1,485	48,481	3.06%
2022 Total	1,281	65,536	1.95%
% Change	-13.74%	+35.18%	-36.19%

* Please note that Taipei Fubon accounts for 5.26% of banking deposit in Taiwan at the end of 2022[1]

Operational Efficiency Figure 2. Project Eagle Eye Model Comparison

	Traditional Rule-based Alerts	Eagle Eye Model
Monthly alerts	57,000	394
Precision rate	0.12%	57.2%
Man-hours per month	2,850 hrs.	32 hrs.

* Please note that there may be a time lag before the police flag an account, meaning that alerts generated by our model at first may be labeled as false positives as they are identified after the fact. As a result, detection rates may appear loTaipei Fubon Bankr for more recent months.

Establishment of Eagle Eye Alliance：Best practice of PPP model in combating digital digital fraud

Since the Eagle Eye Model plays an important role and proved with great performance in combating digital digital fraud, which is a successful trial of the collaboration of the Central police agency and the financial institutions. Thus, instructed by Financial Supervisory Committee and Central Police Agency, Taipei Fubon Bank and other 33 banks in Taiwan (That's the totality of all of the domestic banks in Taiwan)together set up an Eagle Eye Alliance, to implement the Eagle Eye Model into the other 33banks. And by the adaption of each banks to the Eagle Eye Model, each banks can efficiently learn and incorporate an effective model into different bank. Up to date, half of the Eagle Eye Alliance members have completed the implementation of the Eagle Eye Model, and have successfully adjust the model

[1] 2-1 Deposits at General Banks and Credit Cooperatives 2-1 Deposits at General Banks and Credit Cooperatives 2-1 Deposits at General Banks and Credit Cooperatives https://www.banking.gov.tw/ch/home.jsp?id=157&parentpath=0,4&mcustomize=bstatistics_view.jsp&serno=201105120014

to the accuracy of at least 50%(the highest one is 80%), the others are undergoing the implementation process. The Eagle Eye Alliance members have meetings every month to share their experience in the effective counter-measures of digital fraud and experience on the adjust of the original Model. This June 2024, all of the Alliance member banks will share publicly their performance in combating digital fraud.

During this model implementation process, we also found some of the banks, limit to a small scale and the slow path in digital transformation, Ministry of Digital Affairs subsidizes in inviting the resource from the research institute. From the beginning of 2024, National Taiwan University of Science and Technology has participated in the Alliance meeting in assisting 17 of Alliance members to catch up with the implementation of Model and utilize it.

The Eagle Eye Alliance is a best practice of Public-Private Partnership in combating digital digital fraud. In Taiwan's practice, the competent authority(Central Police Agency, Financial supervisory Committee, and Ministry of Digital Affairs), the research institute(National Taiwan University of Science and Technology), and all of the 34 domestic banks are irreplaceable participants.

Section2：Comments and Recommendations

Comments and Recommendation to the draft guidance

- Social media and instant messaging are commonly used by publics nowadays and banks use these as a means of marketing or business promotion. This also provides fraudsters to impersonate the banks'employees or board director by creating fake social media fan pages or accounts.Banks report to social media and instant messaging providers, and request to remove the imposter social media fan pages or accounts in order to reduce the harms. However the providers either take actions inefficiently or ignore completely. Therefore it is recommended to create a platform for banks to report the impersonated fan pages or accounts and the social media and instant messaging providers to take actions on it.
- The Bank recommends BCBS shall establish specific internal control indicators for Financial Institutions to comply with and to fulfill their duties of digital anti-fraud.
- Sharing of Standards for Security Management：The current local regulatory authority has established the "Operational Standards for Security

Management of Financial Institutions Conducting Electronic Banking Services ”for banks. It provides corresponding security design specifications based on transaction risk levels.Given the rapid advancements in technology, it is advisable that any new digital transaction scenarios, verification mechanisms, or regulatory measures in the future be shared among institutions.This sharing would facilitate swift adaptation and real-time adjustments for financial entities.

- Sharing of fraud blacklist：Taipei Fubon collaborates with law enforcement agencies, connecting the blacklist provided by the police currently. This facilitates issuing alerts and implementing preventive measures across all bank channels. It’s advisable to establish fraud blacklists for various countries and industries, recommending an information-sharing mechanism. Through API integration, relevant information can be swiftly synchronized to prevent digital fraud cases in real time.
- Exchange of digital fraud tactics：Suggesting the establishment of a shared platform among countries to address different forms of digital fraud. This platform would enable real-time synchronization of fraudulent transactions, tactics employed by fraud groups, and technologies used. It could also provide corresponding strategies, facilitating financial institutions to access information promptly and develop relevant digital preventive measures within a short timeframe.
- it is suggested that in the future, relevant regulatory authorities could consider or coordinate to implement the spirit and mechanism of bank security standards into the collaboration scope of all electronic payment tools and scenarios, including third-party payments providers and e-commerce platforms to reduce the misusing of customers' payment information.