Taiwan RegTech Challenge 2020

Problem Statements

Summary

This problem statement handout describes the three challenge topics of the “Taiwan RegTech Challenge 2020” and the experience and technical requirements of the participating teams.

Amendments

Version	Date	Amendment Summary
1.0	2020/07/08	Initial draft

I. Background

The Financial Supervisory Commission (FSC) has been actively promoting RegTech in recent years, and its focal points of administration in 2020 include assisting in the financial market's development and addressing consumers' needs for financial services. The FSC continues to build and improve the financial supervision system of Taiwan, and to enhance the international competitiveness of financial institutions. To accelerate the maturity of digital supervision and explore future digital risks, the FSC invited the Taiwan Depository & Clearing Corporation (TDCC), Joint Credit Information Center (JCIC), and associated units to jointly discuss the RegTech development in Taiwan, and also integrated the resources of financial institutions to introduce the latest technologies and systems.

Referencing the UK TechSprint mechanism, the Taiwan Financial Services Roundtable (TFSR) and TDCC organize the first-ever Taiwan RegTech Challenge (TRC) in 2020 and FinTechSpace, TDCC and Institute for Information Industry (III) are the hosts of this challenge.

II. Objectives

To drive the development of RegTech in Taiwan through this challenge, FinTechSpace and TDCC build a strong team, the hosts, for this challenge to promote RegTech development, and have invited experts from across multiple disciplines in Taiwan and abroad to determine practical issues from financial supervision to industrial digital supervision. Calling for mature solutions, experts in the judging panel will select outstanding teams who will then be recognized by the FSC, thereby demonstrating Taiwan's abilities in FinTech innovation, and allowing results to become better aligned with international trends. Objectives include:

1. Identifying feasible methods for accelerating the implementation of RegTech in industries;
2. Building a consensus through the integration of digital supervision across the industry and the government;
3. Connecting to the international RegTech network;
4. Aggregating RegTech capabilities to serve as the competent authority's basis for implementing digital supervision or legal adjustment in the future.

III. TRC 2020 Topics

This challenge takes into consideration the financial supervision practice pain points and needs of the competent authority and the industry for designing the three primary topics and corresponding sub-topics. This is done in the hopes of driving the development of RegTech solutions that can be verified through the one-on-one evaluation after semi-final, and eventually achieve market maturity. The three primary topics include “eKYC,” “monitoring, surveillance & data sharing,” and “fraud prevention/early warning.” The sub-topics corresponding to each topic are as follows:

Item No.	Topic	Item No.	Sub-Topic
1	eKYC	1.1	Primary and premium information process and collection for KYC purposes like electronic identification, strong authentication, etrust services (eIDAS), identity verification, etc.
2	Monitoring, Surveillance & Data Sharing	2.1	Dynamic and automatic real-time data sharing for supervisors and regulators for surveillance relating to operational risk, market risk, sanction risk, etc.
		2.2	Timely incident related information collection and analysis
		2.3	Data sharing in compliance
3	Financial Crime Compliance & Fraud Detection	3.1	Suspicious transactions, accounts and behavior detection for money laundering, financing of terrorism, employee misconduct, etc.
		3.2	Fraud detection
		3.3	Beneficial ownership identification

The corresponding problem scenarios, applied technology and experience requirements for each sub-topic are described below.

Topic 1: "eKYC"

Summary

Currently, when opening an account or making a new financial application in Taiwan, authentication mostly need to be conducted over the counter where the identification and the signature are verified in person for client onboarding. However, as an increasing number of remote financial service scenario and financial service APP, eKYC has become an inevitable trend. An eKYC procedure include processes: identification, authentication and verification. Currently, financial institutes face different pain points in these three processes, such as identification accuracy, authentication object management, information adequacy for verification and KYC process tracking and recording etc. Under such challenging environment and regulatory limits, eKYC methods currently available in Taiwan, like Ministry of the Interior Certification Authority (MOICA) IC card authentication and mobile telecommunication verification, are still limited as MOICA IC card has not been widely used and there are inconveniences in user experience or concerns on potential risks. This challenge topic is proposed for the purpose of improving authentication precision and user experience to achieve non-repudiation of eKYC.

Sub-topic: “Primary and premium information process and collection for KYC purposes like electronic identification, strong authentication, etrust services (eIDAS), identity verification, etc.”

A. Problem description

In response to the advent of the digital age, Taiwan’s financial institutions are inclined to adopt strong identity or transaction authentication tools to meet onboarding

eKYC needs. We welcome local and overseas digital identity solution providers who have cooperated with financial institutions, based on their past experience, to propose diverse solutions that can enhance the protection of high-risk transactions, and that are equipped with features such as the following:

- cardless authentication;
- equivalent to signed and meet in person;
- high-precision biometric identification;
- digital solution applying FIDO or New eID;

to achieve goals like improving the protection of high-risk transactions, resolving the problem of customers not remembering passwords, increasing penetration of MOICA IC card and doing eKYC for disabled etc.

B. Technology and experience requirements

eKYC technologies focused on biometric identification, OCR, image recognition, natural language processing, big data analysis, or research and development of wearable devices.

C. Possible solutions

RegTechs who have previous cooperation experience with financial institutions are welcome to participate. The solution proposed should be applied to at least one of eKYC three stages.

Topic 2: “Monitoring, Surveillance & Data Sharing”

Summary

To reduce supervision disputes caused by market information asymmetry, real-time market monitoring focusing on financial related incidents, such as public sentiment analysis and major incidents reporting, can improve the efficiency of data integration and supervision.

In the disclosure of market information, the competent authority or financial institutions often encounter incidents (e.g. natural disasters, man-made accidents) sparking the necessity to filter out required information from a large amount of data from different sources within a short time to formulate a report. The difficulty lies in integrating multiple data sources (e.g. transaction data, social network data, market data, etc.), which have different data formats like structured and unstructured data. The introduction of technology can not only reduce errors that may be caused by manual operations but also save time and cost.

The key focus that participants must display is how big data analysis and searching techniques been applied to tackle the problem, coupled with machine learning and natural language processing, to semi-automatically assist decision makers in analysis and judgment via data visualization and reporting.

The following are examples of Taiwan’s current practical needs for “Monitoring, Surveillance & Data Sharing”:

- Securities trading are complex and market changes rapidly. Supervisors often need to invest a considerable amount of manpower in handling investors’ accusation or investigating false or misleading market information. In the trading process, if technology can alert securities firms and investors, it would be helpful to alleviate investor concerns.
- In order to identify suspicious transactions and behavior, if industrial data sharing across different institutes and platform integration can be

established, it will be helpful to identify changes in employee investment behavior. If this mechanism is applied to market monitoring changes in collateral prices, financial ratios, business market share and others, it can prevent the occurrence of irrational trading and transactions; thereby, improving the efficiency of risk control of financial institutions. The accuracy of AML system parameters will be improved by analyzing abundant transaction data, so true and false warnings from transaction data can be identified. Furthermore, the characteristic and pattern of abnormal data can be found, and from there, the risk of a transaction being a money-laundering transaction can be calculated.

- Traditional financial institutions have scattered data sources. For the various reports that require to submit regularly in accordance with the law, or the specific data that require to be reported back to the competent authority when certain incidents arise, a lot of manpower is required to gather the data. It is believe that AI and other related technologies can be applied to reduce the manpower cost of data processing.
- The laws and regulations, administrative interpretation, and administrative guidance for financial institutions and other materials of the competent authority are large and scattered information. It is necessary for financial institutions to catch up with changes in financial laws and regulations in a timely manner. Financial institutes should evaluate the scope of impact and the risks of legal compliance, and should determine how to adjust internal regulations accordingly. It is desired that scattered data quick integration and processing and laws and regulations interpretation can be achieved automatically through technology; hence, the efficiency of complying with laws and regulations will be greatly improved.
- Current AML/CFT systems can only perform a

vague comparison of watch lists built internally and externally. When the predetermined threshold is reached, a pending case is raised, which is then judged manually. However, the watch list database often causes difficulty in judgment due to insufficient data. Hence, the staff needs to make additional queries via external news reports and the Sunshine Acts website of the Control Yuan to obtain and compare with extra data, which is manpower-consuming. It is thus favorable to apply site crawler technology to replace manual search and other data comparison and screening technology to reduce the number of misjudgment as well as to ease customers' negative emotion triggered by repetitive inquiries. These help with the reputation, thereby achieving a win-win situation.

Scope of sub-topic: "Early warning of a large number of new account openings in a short period of time," "real-time data reporting and analysis on losses from natural or corporate disasters," "business forecasting under negative corporate news and public sentiment," and "finding suspicious users through cross-domain data sharing and integration." The focus of solutions lies in: (1) Analyzing a large amount of information and promptly generating insights that meet certain conditions, reducing time and labor costs; (2) A visualization of the data and insights that aids analysis and judgment.

Sub-topic 2.1: "Dynamic and automatic real-time data sharing for supervisors and regulators for surveillance relating to operational risk, market risk, sanction risk, etc."

A. Problem description:
When the competent authority conducts the supervision of financial institutions, its main purpose is to monitor the capital market, grasp the financial and operational status of listed and OTC companies. The big data-enabled financial and business reports related to

supervision may contain noises and false data, requiring data cleaning, which requires a large amount of manual processing and affects the response speed of the competent authority towards early warnings on business/market operations. Therefore, this sub-topic focuses on RegTech solutions such as:

- early warning solutions on operational risk;
- early warning solutions on social network and public sentiment;

supplemented with data cleaning tools and false data identification function. These solutions can assist the competent authority in monitoring, early warning, improving administrative efficiency, and reducing manual processing costs, and fit the expected goal of this sub-topic.

B. Technology and experience requirements
Technologies in machine learning, big data analysis, real-time database search, data mining, natural language processing, anonymization, de-identification, UI/UX, visualization, web crawlers, etc.

C. Possible solutions
RegTechs who have previous cooperation experience with financial institutions or in securities markets are welcome to participate.

Sub-topic 2.2: "Timely incident related information collection and analysis"

A. Problem description
When the competent authority encounters natural disasters, man-made disasters, and other incidents that lead to major economic impacts, it often needs to consolidate data from various peripheral units and financial institutions within a short period of time to estimate losses caused by the incident. Therefore, heterogeneous data scattered across multiple supervisory authorities is first converted into structured format, and cross-database data analytics is then carried out in a systematic manner to produce

timely data reports. This improves the administrative efficiency of the competent authority and reduces multiple data processing procedure, which are the expected goals of this sub-topic.

B. Technology and experience requirements
Technologies in machine learning, big data analysis, real-time database search, data mining, natural language processing, anonymization, de-identification, UI/UX, visualization, web crawlers, etc.

C. Possible solutions
RegTechs who have had previous cooperation experience with the competent authority in non-scheduled real-time reporting and file digitalization tools are welcome to participate.

Sub-topic 2.3: "Data sharing in compliance"

A. Problem description
It is often that financial institutions encounter the need to share data across different institutions, e.g. cross-domain (such as financial industry sharing data with telecommunications industry to undertake KYC), cross-industry (such as securities companies sharing data with the banks or insurance companies to undertake client credit verification), intra-industry (such as detecting of any surge in new account openings across different companies in the securities industry), and intra-group (such as the real-time notification of the same customer data within the group, and sharing suspicious transaction information in real time). Therefore, developing automated tools for data sharing in compliance would assist the competent authority, peripheral units, and financial institutions in improving administrative efficiency and internal control quality. This is the expected goal to be achieved for this sub-topic.

B. Technology and experience requirements
Technologies in machine learning, big data analysis, real-time database search, data mining, natural

language processing, anonymization, de-identification, UI/UX, visualization, web crawlers, etc.

C. Possible solutions

RegTechs who have had previous cooperation experience with the competent authority and/or financial institutions in data sharing across different institutes in compliance are welcome to participate.

Topic 3: “Financial Crime Compliance & Fraud Detection”

Summary

Discovering suspicious transaction patterns and illegal service behaviors in banks, securities trading, and insurance, is the primary goal of this topic to achieve fraud early warning. Preventing frauds through effective internal control measures lies on filtering out key suspicious patterns from the vast quantity of operational data and assisting frontline personnel in their judgment during preliminary screening, or even directly making an automatic decision on early warning. Another challenge is that there are countless and continually changing patterns of fraud; hence, intelligently self-discovery and self-learning new suspicious patterns from ample information is wanted.

The key focus of this topic lies in applying big data technologies, like artificial intelligence, machine learning, and natural language processing technology, to automatically or semi-automatically assist decision makers in fraud analysis through visual means.

The following are examples of Taiwan’s current practical needs for “Financial Crime Compliance & Fraud Detection”:

- Default under syndicated loan have caused big amount of financial losses for the related lenders. If early warnings on cooperate borrowers’ financial or operational changes, or post-loan risk management can be done automatically and properly, it will be helpful for risk control. This technology can also be applied to general loans.
- In response to misconduct of business personnel such as malpractice or assisting customers with fraudulent insurance claim, if technology can help business personnel to analyze insurance purchasing behavior on solicitation and insurance

products, and issue early warning notices for unusual behaviors / patterns (such as when there is a high rate of high-risk customers being solicited or high rate of clients been reported as suspected money-laundering accounts).

- For unusual financial behavior such as heist and fraud, macro-level of guidance is required. If financial institutes can get access to and analyze cross-domain data from telecommunications, other financial or non-financial authorities, etc., financial institutions would have more room for fraud detection use case application and technology development.
- In terms of anti-money-laundering, financial institutions currently use dedicated suspicious transaction reporting devices, which must have a fixed IP and no access to external domains, in accordance with laws and regulations. If a RegTech solution / technology that can also provide information security measures to reduce the risk of hackers, it would allow financial institutions to avoid using a dedicated device for suspicious transaction report and the inconvenience this caused.

Scope of sub-topic: "Detection of abnormal transaction behavior and pattern" and "AML/fraud/information security integrated internal control solution." The focus of solutions lies in: (1) Analyzing a large amount of information and promptly generating insights that meet certain conditions, reducing time and labor costs; (2) A visualization of the data and insights that aids analysis and judgment.

Sub-topic 3.1: "Suspicious transactions, accounts and behavior detection for money laundering, financing of terrorism, employee misconduct, etc."

A. Problem description

Identifying malpractice and misconduct in financial

institutions is mainly divided into internal fraudulent behavior detection and external suspicious transaction/account detection. An internal malpractice detection mainly corresponds to telemarketing monitoring and order spoofing detection. External malpractice identification pain points correspond to improving the accuracy of detection of fraudulent behavior, heist, detecting insurance/fraudulent insurance anomaly, identifying dummy account, and identifying emerging risk patterns. It is expected that solutions from this sub-topic can reinforce financial crime prevention and control, improve the quality of internal control or strengthen corporate digital legal compliance capabilities. Also improving the accuracy of anomaly detection via technology, and discovering emerging risk patterns are preferred.

B. Technology and experience requirements
   Technologies in machine learning, big data analysis, social network analysis, data mining, natural language processing, UI/UX, visualization, web crawlers, or wearable devices, etc.

C. Possible solutions
   RegTechs who have had previous cooperation experience with financial institutions and have mature solutions ready for verification and explanation are welcome to participate.

Sub-topic 3.2: “Fraud detection”

A. Problem description
   Defaults in the securities transactions and loans of financial institutions is the common pain points for the regulator and financial institutes. Technologies that reinforce the function of fraud detection and early warning are desired; hence frauds can be effectively decreased. In addition to improving the accuracy of behavior representation for fraud detection in securities transactions, it is necessary to do the post-loan credit monitoring on the borrower on social

network discussions, public opinion and negative news. The solution is expected to improve the accuracy of unusual behavior detection, monitor the trading market intelligently, reinforce financial crime prevention and control, and manage credit risks effectively.

B. Technology and experience requirements
Technologies in machine learning, big data analysis, social network analysis, data mining, natural language processing, UI/UX, visualization, web crawlers, or wearable devices, etc.

C. Possible solutions
RegTechs who have had previous cooperation experience with financial institutions and have mature solutions ready for verification and explanation are welcome to participate.

Sub-topic 3.3: “Beneficial ownership identification”

A. Problem description
When a financial institution monitor customer deposits and other transactions to ensure they aren't part of a money-laundering scheme, the most important task is to identify the beneficial owners in the transaction. In addition to trace the internal transaction trails of the business, it is also necessary to create a relationship network in accordance with the transaction context from which related accounts are then be classified. The identification of the beneficial owners is expected to reinforce financial crime prevention and control, improve the quality of internal control, and strengthen the digital legal compliance capabilities of financial institutions.

B. Technology and experience requirements
Technologies in machine learning, big data analysis, social network analysis, data mining, natural language processing, UI/UX, visualization, web crawlers, or wearable devices, etc.

C. Possible solutions

International RegTechs, who have had previous cooperation experience with financial institutions in identifying beneficial ownership in money laundering prevention and control in a MVP or a prototype, are welcome to participate.