TOWARDS INCREASED EFFICIENCIES IN KYC AND TDD SCREENINGS

INTRODUCTION

Banks are subject to an increasing regulatory pressure relating to various regulatory regimes, such as anti-money laundering ("AML"), economic sanctions and export controls. To mitigate potential liability, banks regularly invest resources in screening their customers and their customers' transactions, a procedure that is normally referred to as Know Your Customer and Transaction Due Diligence Screening ("KYC/TDD"). As many customers often engage with more than a single bank at a time, the efforts of these banks, with respect to KYC/TDD, are often duplicative. They are conducted separately by several banks with minimal-to-none cross-banks coordination. This working paper explores the pitfalls of the currently applied duplicative system of KYC/TDD and proposes a coordinated system that may substantially reduce KYC/TDD procedure costs and improve overall efficiency. We subsequently describe the process side of the system and analyse potential challenges.

EXECUTIVE SUMMARY

As banks and customers alike begin to recognise the importance of improving operational efficiencies and increasing customer satisfaction when conducting KYC/TDD, the IFFC's Compliance Chamber has developed a third-party KYC/TDD vendor model, designed to save some of the resources lost as part of a duplication of efforts exerted by various banks to gather similar sets of information regarding their customers.

Over the past several years, many proposals of market utilities for KYC/TDD have emerged globally. We propose engaging an existing or a newly created vendor (or a consortium of vendors) to standardize the KYC/TDD processes and ensure smooth customer on-boarding and regulatory compliance. This would be done by centralising both customer information and related documentation into a secure repository. Banks subscribing to the system would be able to access the centralised database in relation to their prospective customer and leverage the information to further perform enhanced risk management. With this information, banks would be able to decide on whether to engage in transactions with the customer, thereby reducing the overall operational costs.

KYC/TDD: THE PROBLEM OF DUPLICATION OF COSTS

Role of KYC/TDD in combatting financial crimes

Banks are required by laws and regulations to perform KYC/TDD screening on their customers and their customers' transactions. In order to comply with a myriad of regulatory requirements and mitigate risks, banks perform KYC. Furthermore, banks — depending on the levels of risk associated with a transaction — conduct TDD to assess the customer risk as well as to determine the customers' transactional risks in certain geographical, sectoral, product and tax areas, and to identify irregular and suspicious transactions.

Briefly, this process entails extensive due diligence to identify the trustworthiness of prospective customers and to obtain relevant information necessary for doing financial business with them. The growing pressure in the financial industry and the increase in customer expectations means that the compliance function has never been more vital to banks and other financial organizations in terms of offering an efficient customer on-boarding experience, while at the same time detecting criminal activity and deterring people and businesses from engaging in criminal activity. The KYC/TDD processes serve as the first line of defence for banks when screening potential customers, having great implications for not only the bank's bottom line, but also its reputation. The KYC/TDD processes may shield banks from money laundering, terrorist financing and other related threats to the integrity of the international financial system and ensure that banks engage with reputable and compliant customers. However, a bank's ability to

do this is largely influenced by the data it can gather on prospective customers, the efficiency of the data-gathering process, and industry-related laws and regulations that it is required to comply with.

Offenders are becoming more specialised in their criminal activity, leaving authorities with increasingly complex questions and more sophisticated investigations. Laws and regulations across the industry are constantly evolving in order to ensure that banks are able to effectively identify, verify and monitor their customers and their customers' financial transactions, to prevent money laundering and the financing of terrorism. The financial industry has undergone ample shifts since financial regulators increasingly began to focus on enhancing the level of sophistication of KYC/TDD. Despite those changes, the complex laws and regulations are far from being standardised and leave substantial room for interpretation by individual banks.

Inconsistent KYC/TDD processes

Banks are subject to a wide range of regulatory frameworks such as the Fourth EU Money Laundering Directive (4MLD), the Financial Crimes Enforcement Network's (FinCEN) Final Rule on Beneficial Ownership, anti-bribery, anti-corruption and AML laws. KYC/TDD screenings are an important tool for banks to ensure compliance with such regulations. Screening, for instance, assists in: identifying customers and verifying identities against numerous external publicly-available databases; identifying the ultimate beneficial owner ("UBO") and verifying the ownership and control structure of the customer; obtaining information on the purpose and intended nature of the business relationship; and scrutinizing the transactions being conducted to ensure that these are consistent with the business and risk profile of the customer.
To date, many financial market organizations have issued guidance and manuals with the goal of introducing a comprehensive KYC/TDD screening framework (e.g. the "FATF Recommendations"). Nevertheless, in practice, there seems to be no widely accepted 'golden standard' that is being followed by all banks: each bank applies its own internal procedures and standards to the best of its interpretation of all applicable regulations.

Duplication of efforts

KYC/TDD screenings undertaken by banks are costly. According to a recent survey, banks currently spend over USD 60 million on KYC/TDD screening annually. By 2018, a quarter of all banks — with total assets between USD 101 billion and USD 500 billion — expect their expenditure on AML activity to increase by over 50 percent. Some of the high costs are the result of embedded challenges in KYC/TDD processes, including :

- Lack of automation: Businesses manually process the data received from customers for the KYC/TDD screening. Manually processing data creates many problems such as resource drain, data quality problems, expanding costs and delays in completing the KYC/TDD process.
- Drain on resources: The manual processing of information takes large amounts of time and human resources and requires the diversion from other tasks towards KYC/TDD.
- Data quality: The manual processing of data can cause misinterpretation or loss of data, which is highly dangerous for the KYC/TDD for AML purposes. Especially in large banks which work with large corporations, assuring data quality is a challenge, even disposing of the best task force to handle the data.
- Customer expectations: Running an enhanced KYC/TDD is timely and costly. However, customers of large banks also expect to be on-boarded with the banks as quickly and effortlessly as possible in order to run their businesses. Even though large corporations are aware that the banks must run the KYC/TDD processes in order to comply with AML regulations, delays create a negative impression and the feeling of not being trusted while doing business with the chosen banks.

- Risk profiling: It is increasingly challenging for banks and KYC/TDD professionals to assess whether existing or potential customers pose regulatory risks.

While KYC/TDD costs are substantial, under the current state of affairs, each bank conducts a new screening per customer. This means that it has no access to valuable factual and background material that may have recently been collected by another bank for the same customer. This duplication of efforts (and costs) is underscored by examining the results of another survey, showing that corporations have, on average, relationships with 10 banks globally, with larger corporations having as many as 14.

The parallel KYC/TDD procedures conducted by different banks on the same customers not only slows down on-boarding procedures by banks, but it also generates unnecessary duplication of costs, thereby increasing the overall costs of the system and possibly jeopardising the smooth functioning of the system. In practice, the lack of standardization and cooperation between banks has severe repercussions in terms of speed and efficiency for both the customer and the bank. It may not come as a surprise that over 50% of large banks expect an increase in spend for AML activity between 25% and over 100%.

ENHANCING EFFICIENCIES: A PROPOSED VENDOR MODEL

Proposal

In this white paper we consider the creation of a centralised system run by a vendor or a consortium of vendors, which collects KYC/TDD information from (potential) customers and their transactions based on a widely agreed standard. Broadly, this system would secure access to all banks participating in the system through subscriptions, and the information collected with respect to customers would be available to all participating banks. Figure 1 describes the proposed structure of the system:

Figure 1: Vendor model

As several initiatives of a central repository have emerged recently, this working paper proposes the engagement of a vendor (or a consortium of vendors) that is credible and trustworthy.

The proposed framework is designed to be collaborative, transparent and efficient. It aims to create a level playing field, as information will be shared equally among participating banks. When subscribing to the vendor model, banks would no longer need to collect their own information on each customer. Instead, the collection of information would be done by a vendor (or a consortium of vendors) on behalf of the bank.

Below we list some of the features of the proposed framework:

- The vendor model is based on the creation of a common KYC/TDD standard, which is accepted across the industry. This standard could also be developed by the regulators or vendor, or otherwise. The vendor collects the information based on a standardised form that would meet regulatory requirements and market standards.
- The collection of information is done in direct contact with the customer, and the costs are borne by the customer.
- The information is made available to all subscribed banks equally and simultaneously.
- The vendor prepares a KYC/TDD report for each corporation and ensures standardisation across the market. The vendor makes the KYC/TDD data available to all network participants, who pay a subscription fee to receive such information from the vendor.
- The information collected by the vendor is presented in a report, and includes a high-level, objective risk assessment based on a transparent matrix.
- The vendor is responsible for performing quality checks, regular monitoring and the carrying out of audits in order to ensure that the information is reliable and up-to-date. The vendor periodically updates the information collected on the customer.
- The vendor creates a common, central database of whitelisted combinations of companies and transactions, and keeps the database as up-to-date as possible.
- To ensure the collaboration of the subscribing banks, the system contains penalties, such as blacklisting, for potential customers who deceive or attempt to deceive the system.
- The vendor must be a credible and trustworthy third party which operates in a transparent way and which is of the same distance to all network participants. The vendor bases its operations on standards and principles agreed upon by all network participants, and there is no doubt about the vendor's transparency or reliability.
- The vendor is subject to regulatory oversight in order to assure the vendor's compliance with existing regulatory requirements and to ensure the maintenance of high quality of KYC/TDD data provided to the market.
- The vendor is audited by a reputable independent auditor annually. The audit report is made public.
- Currently, banks carry out all KYC/TDD responsibilities themselves. With the creation of a vendor model, banks would remain accountable, but certain responsibilities would be outsourced to the vendor. The KYC/TDD responsibilities can essentially be divided into two broad categories: (i) data collection; and (ii) initial risk assessment. The following sections will analyse the responsibilities pertaining to each category in order to determine the delineation of duties between the banks and the vendor.

Data collection

The tasks relating to data collection would be outsourced to the vendor. The first and main task of the vendor would be to collect the KYC/TDD data from each (potential) customer, as required by the regulations. Other interrelated responsibilities that could be outsourced to the vendor include, amongst others, performing database management (including '"expiry dates"); executing daily cross-checks of blacklists; scanning for open-source data relevant for risk evaluation; interpreting and enriching collected data to the level of information and knowledge; supplying required data and information to banks; and notifying when the situation changes in an open case, including any changes in the blacklist or the publicly-available data. If the data is already available in the vendor's database, the vendor would verify the accuracy of the data and confirm its accuracy before sharing it with the bank.

The vendor would directly collect the required data for the KYC/TDD from the customer, and the customer would pay for the KYC/TDD costs. All banks within the financial services sector would purchase their KYC/TDD information from the same vendor (or a consortium of vendors) which would provide this information in a timely and standard manner.

The vendor would securely store the data in its database, remain in contact with the customer and ensure that the data is updated periodically. The vendor would monitor the customer data to detect changes, automatically refresh the information, and report any change in KYC/TDD data to banks.

Given the ever-changing character of regulations, the vendor would also remain apprised of necessary regulations. Any updated procedures observed by the vendor would made be made available to all participating banks at all times.

Importantly, the services provided by the vendor are not to be considered a substitute for banks' responsibilities — the main aim of having a vendor model in place is to facilitate the KYC/TDD activities of banks by collecting data and standardising the process. Banks may decide not to rely on the information collected — or the risk assessment conducted — by the vendor, and carry out any additional screening actions without bearing any duty to feed the outcome of its analysis back to the joint platform run by the vendor.

Initial risk assessment

It is our view that the services provided by vendors should, as a first step, be limited to basic KYC/TDD competencies. However, we expect the vendor model to be expanded to eventually include more advanced KYC/TDD elements. In that case, this enhanced vendor model could, for instance, perform an objective analysis based on pre-agreed criteria. They could also deliver to banks an initial indication of the risk involved in a contemplated engagement or transaction.

In a system where the vendor is also assigned with the task of performing a risk assessment, a large portion of the KYC/TDD process would be shifted from the banks to the third party. Eventually, this would substantially reduce the costs of the KYC/TDD process and ensure a better level of standardization.

If the vendor is assigned with risk assessment tasks, the vendor would perform this task in addition to the data collection, storage and distribution tasks, as illustrated above. The vendor would accommodate a team of expert KYC/TDD professionals to verify customer data, determine the UBO and assess the potential risks / non-compliance with AML regulations.

The results of an enhanced KYC/TDD which is performed only once and run by a professional and centralised KYC/TDD team and AML experts within a specialised vendor would inherently be more reliable, accurate and consistent with the ever-changing reality.

In addition to periodic information reviews, at the request of a specific bank (and for a fee), the vendor would regularly screen media and publicly-available sources to monitor the customer and its activities. The aim should be to ensure real-time customer monitoring to support strong AML compliance. Upon a bank's request (and for a fee), the vendor would conduct event-based customer reviews, following any trigger event deemed suspicious by the vendor or AML regulations. Changes in executive management or in the shareholding structure, business expansion to new countries considered risky for AML purposes, IPOs, expiry of certain documents or the emergence of negative media coverage on the customer could be seen as trigger events to re-run an ad hoc KYC/TDD review on the customer to maximise AML compliance. In this case, the relevant vendor KYC/TDD team would notify the relevant banks which have already purchased KYC/TDD data on this particular customer. The banks would then assess the new information and take necessary measures to ensure compliance with AML regulations.

Clearly, if the vendor is granted with risk assessment tasks, it would benefit banks as (i) the customer data would be processed by a highly skilled, well trained and experienced KYC/TDD team minimising any data misinterpretation risk, (ii) both the assessment of data and the reporting to the bank would take place in a

standardised manner, thereby making it easier to process, (iii) banks would save both on manpower and costs which would otherwise be dedicated to KYC/TDD.
As mentioned above, the services provided by the vendor are not to be viewed as a substitute for a bank's responsibilities. Even if the vendor performs a risk assessment analysis, the analysis does not free the bank from its liabilities.

Automation

According to Thomson Reuters, the average firm currently spends USD 60 million per year on KYC/TDD activities. Furthermore, manually processing KYC/TDD data is prone to errors (human error can lead to the misinterpretation of data while processing vast amounts of sensitive data), jeopardising the ultimate goal of KYC/TDD: full compliance with AML regulations.

It is generally agreed that technology is a key component for optimising KYC/TDD processes and procedures. According to recent trends, whenever possible, manual intervention to the KYC/TDD process should be avoided and replaced by credible and reliable automated systems.

Given the complexity of financial regulations and its fast changing nature, in addition to the actual data verification process, customer on-boarding is becoming increasingly time consuming. For example, it took banks 32 days on average to on-board a new customer in 2017, as compared to 28 days in 2016. Customers are reluctant to conduct further work with banks when their on-boarding time increases. Recent surveys show that the lengthy KYC/TDD process caused 12% of a total of 1,122 participating respondents to abandon their banking relationship and seek to engage another bank. Automation would not only be efficient in assuring better compliance with AML regulations, but would also expedite the customer on-boarding process and would benefit the financial industry as a whole.

Data protection

With the vendor responsible for storing the privileged, sensitive and confidential data of many customers, the vendor must respect strict data security requirements when handling such data.

Pursuant to our proposal, banks would obtain KYC/TDD information on specific customers whenever a potential business relationship is in the process of being established with a customer, and when the customer also consents to the processing. The goal of the process is to be fully transparent, with the customer receiving a detailed privacy notice.

The vendor would hold the customer data confidential at all times, and would take necessary measures to prevent the data from leaking. The vendor would also ensure that it complies with national and international data privacy and protection rules, and securely share KYC/TDD information with banks.

Whitelisting and Blacklisting

Pursuant to our proposal, the vendor or a consortium of vendors would perform KYC/TDD on behalf of the banks. As explained above, the vendor would mostly have data collection tasks, such as: performing database management; executing periodic checks against blacklists and public databases; scanning for open source data relevant for risk evaluation, interpreting/enriching collected data; supplying required data/information to banks in a standardized format; and notifying relevant banks when there is any change in data, blacklists or public databases which concerns the customer.

In the near future, the vendor could also be asked to perform a portion of the risk assessment depending on the amount of assessment and intelligence required. However, in principle, the following responsibilities are vested in banks: performing complementary research if the available information is not sufficient; evaluating against own risk appetite; and concluding whether the bank can engage in the transaction. Avoiding, mitigating, transferring or accepting the risks revealed as a result of the KYC/TDD is also the responsibility of banks. Certain types of tasks within the risk assessment (such as the preparation of and

following up with checklists) can be transferred to the vendor, whereas some more complex tasks (such as face to face interviews) must be performed by banks.

The vendor, during the course of the KYC/TDD, will be in an ideal position to identify and report red flags on the customer. By doing so, the vendor could provide the banks with a whitelist and a blacklist of customers who seem to comply with the AML regulations and vice versa. The whitelists and blacklists created by the vendor should not, under any circumstance, be considered as the basis for pursuing or not pursuing transactions with such customers. However, these would be helpful for the banks' internal KYC/TDD teams, as they would provide a first impression of the customer and would assist banks in determining the level of scrutiny in their own risk assessment.

Benefits of the proposed vendor model

Outsourcing the KYC/TDD process to a centralised third party, namely a reliable vendor that banks agree on, would not only be innovative but also beneficial for both customers and banks. Our suggested model directly ties in with the challenges of the current approach described in section 3, and may dramatically reduce costs and inefficiencies.

Banks would become members of the network by paying a subscription fee. They would gather their KYC/TDD data directly from the vendor (or a consortium of vendors) instead of the customer. Ideally, the costs of the KYC/TDD would be borne by the customer. The vendor (or consortium of vendors) would also be in charge of periodically updating the KYC/TDD data collected in cooperation with the customer, eliminating the need for banks to perform KYC/TDDs each time they engage with the same customer. The proposed system with a centralised vendor (or a consortium of vendors) would be undoubtedly more cost efficient relative to the current situation in which each bank performs separate KYC/TDD on the same customers.

In addition, banks are currently not able to share information on suspicious individuals or entities and are thus unaware of previous suspicious activities. A centralised mechanism that stores information on suspicious individuals or entities would increase transparency and awareness in the market in relation to suspicious activities and limit the possibilities for money launderers to easily switch to a new institution.

Performing KYC/TDD is costly for both customers and for banks. In our proposal, customers would not have to experience a costly and time-consuming KYC/TDD each time they engage with a different bank. Rather, the costs of the KYC/TDD would only be borne once. The data collected from the customer would then be shared by the vendor with each bank. The customer on-boarding times would decrease, benefiting from automation in KYC/TDDs, and overall customer satisfaction would increase.

The vendor would be a KYC/TDD professional company. The employees of the vendor would be highly skilled, trained and sector specialised KYC/TDD professionals performing KYC/TDDs on a much more focused and customer-oriented level. The chances of data loss or misinterpretation would decrease visibly. The duplication of effort would be reduced, since all data would be collected and analysed by one vendor (or a consortium of vendors) in the market based on a standard model. Standardisation across the market would facilitate the KYC/TDD professionals' work within the banks and increase the overall quality of analysis.

The vendor would use advanced technology and specifically automation in order to process the data received from customers. It would develop necessary software to be able to process larger amounts of data within a shorter time span. Automation would eliminate manual regulatory data collection and analysis. The quality of the collected data and the analysis would increase since the margin for errors would decrease with the automatization of the system. Banks would be able to spare the manpower they used to dedicate to basic KYC/TDDs and channel it to more advanced follow-up screening activities.

The vendor would be fully aware of the changing regulation and work with the relevant regulatory authorities in order to keep track of the changes in laws and regulation, therefore a better AML compliance would be established within the financial sector.