Issue No. 5
December 2020

Regtech Watch is a newsletter published by the Hong Kong Monetary Authority to promote the adoption of regulatory technology (Regtech) by the banking industry. It provides information on actual or potential Regtech use cases rolled out or being explored in Hong Kong or elsewhere. The objective is to assist authorized institutions (AIs) in adopting innovative technology to enhance their risk management and regulatory compliance.

Background

This fifth issue of Regtech Watch focuses on how greater technology adoption has enabled AIs to maintain business continuity and effectively respond to the various operational challenges presented by the COVID-19 pandemic.

It should be noted that the sole purpose of this newsletter is to provide AIs with information on the latest Regtech developments. The HKMA does not endorse any use cases or solutions described in this newsletter. If an AI intends to adopt a particular solution, it should undertake its own due diligence to ensure that the technology is suitable for its circumstances.

Regtech in response to COVID-19

Key challenges

With Hong Kong having experienced multiple waves of COVID-19 over 2020, the Government is adopting an agile approach (i.e. the "Suppress and Lift" policy) to relax and tighten social-distancing measures in accordance with latest developments. During times where strict social-distancing measures are called for, the HKMA will remind banks to take suitable steps to protect their staff and customers, including allowing their employees to work from home where possible. This inevitably means that certain banks have had to close or shorten the operating hours of their branches and introduce extensive work-from-home arrangements. Various operational challenges to banks may have surfaced during

these times, including how to quickly transition and have staff embrace digital working methods, ensure sufficient monitoring of employee-client communications for compliance purposes, and provide employees with remote access to internal databases and systems without compromising security.

Besides managing the immediate challenges presented by work-from-home arrangements, banks also need to remain vigilant to the risk of COVID-19 infections even after the pandemic situation eases and physical operations are able to resume. These involve considering ways to monitor employees' or customers' potential exposure to confirmed infection cases and how to lower the risk of transmission at offices and branches by better enforcing social-distancing measures.

How can Regtech help?

Technology can play a major role in helping address the operational challenges mentioned above. As the use cases below demonstrate, it can, for example, smoothen the process of transitioning staff to a remote working environment by supporting communication channels and work processes that mimic, or even augment, those available in-person or at the office. Furthermore, technology can also be deployed to enable more systematic and efficient surveillance or contact tracing that manual methods would not afford.

It should be noted that while some of the technology solutions being put in place may indeed be temporary and specifically tailored to COVID-19, the banking industry's general pivot towards technology and digital transformation has long been underway. Banks may wish to consider whether any of these arrangements can be permanently adopted as business-as-usual arrangements.

Regtech use cases

The HKMA has observed four potential Regtech use cases that may be relevant to COVID-19. The details are summarised below for reference in the following boxes.

Use case 1 – Remote access and collaboration platforms

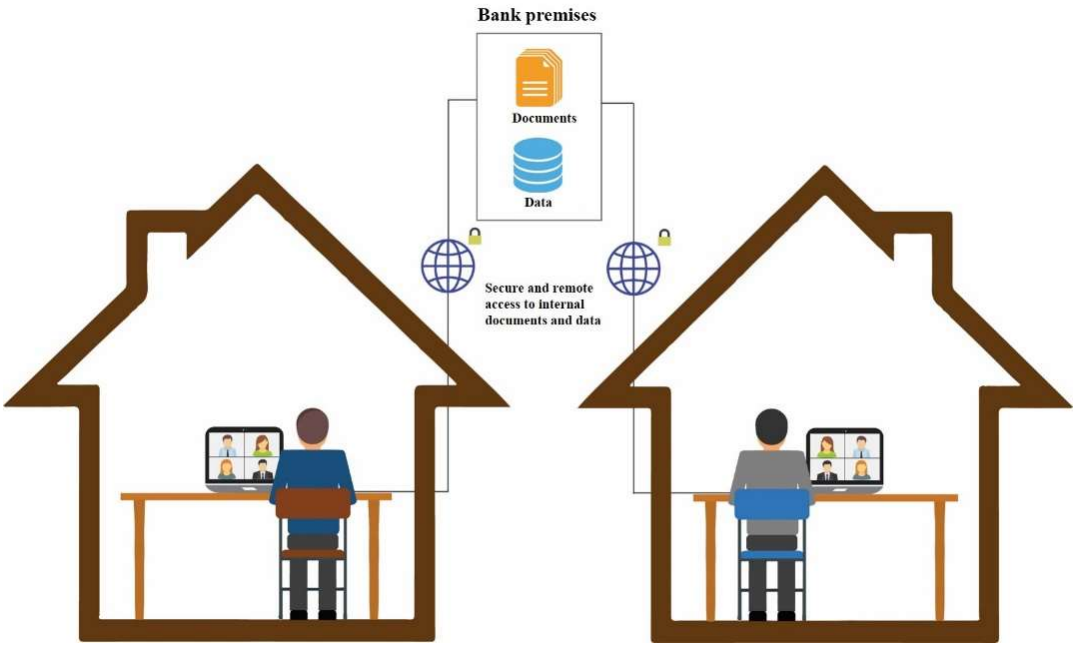
The necessity to implement work-from-home arrangements has highlighted to banks the need to re-consider the sustainability of purely traditional ways of working, including reliance on on-premises access to applications, data, and files, and face-to-face meetings. While it is clear that some degree of digital transformation is required, banks should, in undertaking this journey, stay alert to such risk management considerations as how to remain compliant with regulations, whether sensitive information is sufficiently protected, and whether adequate access controls and identity verification measures are in place. System stability and business operational continuity should also be ensured as remote access is rolled out on a large scale.

Taking all this on board, some banks are deploying a range of technology solutions to support remote working in a scalable, sustainable and secure way. For instance, video conferencing solutions, fortified with additional security settings, including end-to-end encryption, are widely adopted by banks to ensure that all kinds of meetings can be held no matter where employees are situated. Some video conferencing solutions also support on-premises hardware security modules for extra data security as well as digital archives of encrypted communications for compliance and record keeping.

Besides, to maintain the operations of different data-dependent banking functions (such as those performing risk management model recalibration and meeting regulatory reporting requirements), banks are also working to resolve the issue of on-premises and decentralised data repositories, which would otherwise be inaccessible during times of remote work. Accordingly, some banks are moving to store certain data on centralised and cloud-based data management solutions such that employees can securely and remotely access the latest internal data while achieving better operational resilience. These solutions also allow banks to migrate their data models to cloud platforms which offer additional scalability, and can help banks meet unforeseen demand for ad-hoc and computational-intensive data analytics, such as risk model adjustments that arise as a result of COVID-19.

Ultimately, these solutions enable banks' staff to collaborate and work in a remote and safe manner, but without compromising the banks' business and operational continuity.

Exhibit 1: Secure virtual meeting and remote data access



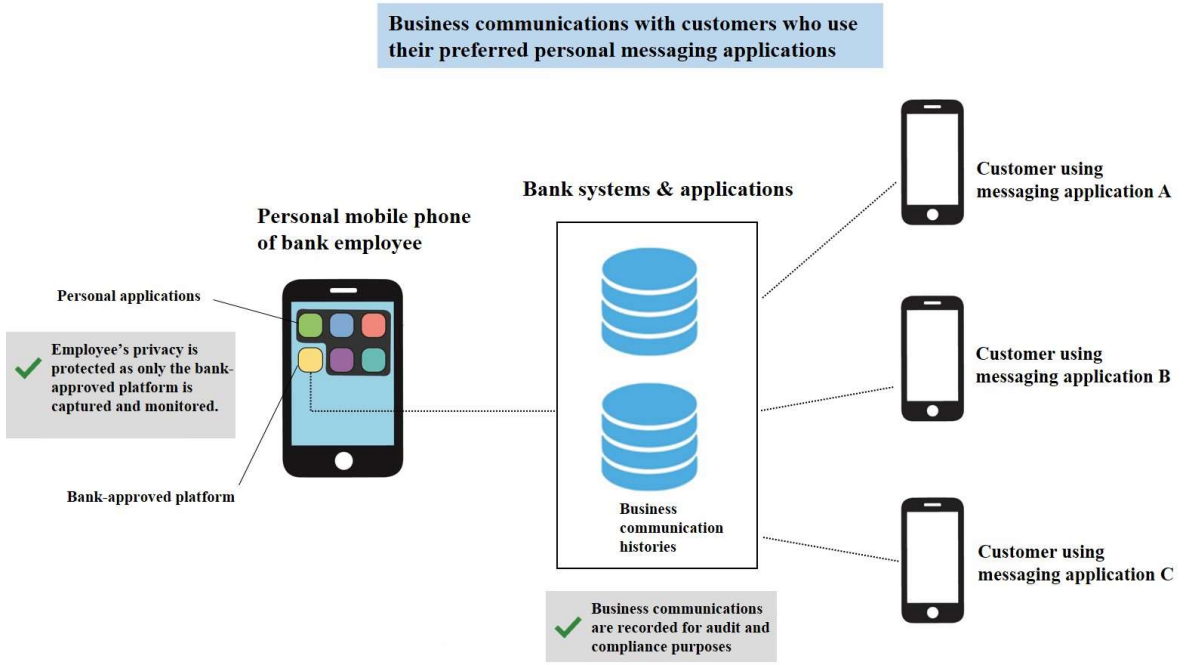
Use case 2 – Enabling compliant business communication

As work-from-home arrangements are activated within a short notice period, not all banks are technically prepared to enable employees to have remote access to certain internal systems (e.g. email systems). As a result, bank customers may have turned to personal messaging applications (e.g. WhatsApp and WeChat) in order to discuss business issues with their regular bank contacts (e.g. relationship managers). The use of personal messaging applications creates operational challenges as banks have no visibility nor means of capturing and archiving the dialogues between their employees and customers for audit and compliance purposes in order to comply with relevant regulatory requirements.

Some communication solutions may potentially solve this issue. These solutions provide an all-in-one enterprise messaging platform, which is compatible with common personal messaging applications through different

technical connections (e.g. application programming interface (API) gateways) as well as with certain popular corporate tools. In other words, employees can use a single, bank-approved platform to communicate with customers. These customers can still use their preferred personal messaging applications and are not required to install any additional application to interact with the banks. Given that all communication passes through the standalone and dedicated messaging solution managed by the bank, all business communication histories can be recorded for audit and compliance purposes (e.g. employees cannot delete the communication records on their own mobile phones) without sacrificing customer experience. These solutions come with the added benefits of integration with other business critical applications as well as allowing banks to only monitor those communications related to business. This should alleviate employees' concerns that their personal communications will be subject to monitoring, while at the same time ensuring banks' compliance with regulatory reporting and other regulatory requirements.

Exhibit 2: Separation of personal communications from business usage that require monitoring



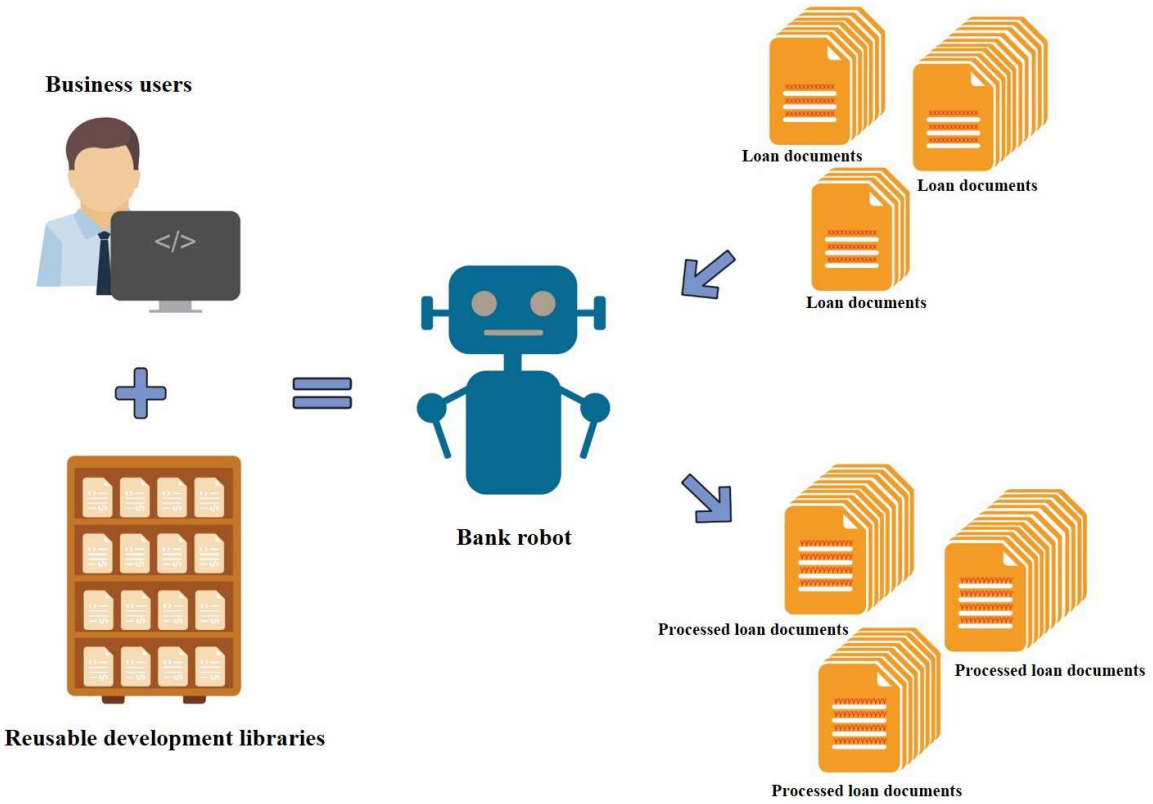
Use case 3 – Automating the process of granting COVID-19 relief

COVID-19 has led to a significant reduction in economic activities and put financial pressure on a number of industries. In order to tide over businesses during this difficult time, authorities around the world, in coordination with financial institutions, have introduced various financial relief measures. For instance, the HKMA worked with banks to introduce the Pre-approved Principal Payment Holiday Scheme, which defers principal payments owed by corporate borrowers for up to 12 months.

Although the framework for relief is in place, it is crucial that banks are able to process relevant documentation and formalise the arrangement in a timely manner to alleviate businesses' cash flow pressures. While this is – given the tight timeframe – already an onerous task, it can become even more difficult when combined with work-from-home arrangements, during which less manpower may be available to assist with manual and repetitive tasks.

In order to overcome this, banks are utilising robotic process automation (RPA) to perform time-consuming and repetitive work on a 24x7 basis, and streamline the process. For example, the robot will pick up the borrowers' applications from a system, determine if the borrowers' loans are valid for payment postponement through whitelist checking, modify the payment terms in each of the relevant loan documents, and send letters of confirmation to the borrowers. Given business conditions can change quickly under COVID-19, it is crucial that such RPA applications can be deployed in a flexible and nimble fashion, cutting through the complexity of protracted system development cycles. In this connection, some banks have decided to enable and empower its business users to take charge of their own RPA deployment. With the help of their RPA vendors, these banks have established teams of business users, who are individually empowered to build robots to automate processes, and developed reusable development libraries which enable swift robot design and deployment in accordance with rapidly changing business needs. This automation of processes aims to reduce operational risks by limiting the possibilities for human or manual errors, especially when staff are under pressure to process large amounts of documents in a short period of time, and without the usual convenience or support available in an office environment.

Exhibit 3: Empowering RPA development to streamline loan document processing



Use case 4 – Social-distancing and contact-tracing solutions

Social-distancing requirements can range from the more extreme mandatory lockdowns to less intensive measures, such as those which establish limits on group sizes or minimum physical distance to be maintained between individuals. Hence, even when banks are able to resume physical operations, they may still need to enforce certain social-distancing requirements or take steps to manage the risks of COVID-19 infections, including for example through contact tracing.

While social-distancing guidelines can be enforced manually, some potential technology solutions can do so more effectively. With the assistance of artificial intelligence (AI) and the Internet of Things (e.g. AI-powered three-dimensional

cameras with spatial and depth perception), these solutions can continuously collect visual footage and statistical patterns or spatial data, and analyse the collected data to measure the distance between customers. Timely alerts will be provided to effectively identify any cases that breach the social-distancing requirements (e.g. customers are standing too close to each other while queuing for teller services at the branch) and require remedial action. Such real time and accurate spatial analysis has an evident advantage over traditional closed-circuit television systems, which lack the ability to capture pictures augmented with three-dimensional spatial information.

As physical operations resume, some banks may also consider reducing the proportion of staff working from home. However, as responsible employers, banks must ensure that in doing this, they are able to provide a safe working environment for staff, and have the ability to alert staff if there are signs that they may have come into contact with potential or confirmed COVID-19 cases. As an alternative option to social-distancing solutions, there are emerging innovative solutions, which can advise how closely or for how long an infected employee may have been in contact with other employees. One such solution makes use of the electronic signals (e.g. Bluetooth and Wi-Fi) of mobile phones and proximity data, combined with various advanced techniques (e.g. tagging and geofencing) to reconstruct the contact histories of employees in offices. Tagging allows companies to identify individual employees through unique identifiers associated with their mobile phones, and geofencing relies on the coverage of various electronic signals to determine whether an employee has a history of entering certain areas of the workplace. By analysing signals received by a mobile phone from other nearby mobile phones and their location data, the solution can estimate the distance between employees in the office at any given point in time and the duration of any close contact. Therefore, companies can immediately identify and advise those higher-risk employees to undergo self-isolation.

Since these solutions collect personal data, they can only be successfully implemented with the buy-in of employees and customers. To this end, banks should obtain adequate support from employees before rolling out the solutions in the workplace and consider developing a well-defined exit strategy before launch. The exit strategy reassures employees that the tracing is only a

temporary measure in response to the pandemic situation. Further, banks should also consider establishing a clear communication plan to help explain the purpose and operation of the solutions, and address employees' and/or customers' concerns about how their personal data will be used and handled.

If successfully deployed, these solutions can offer senior management the insight required to make more informed and risk-balanced decisions when responding to confirmed infection cases. This benefits operational resilience and lowers the possibility that unnecessary office closures causing operational disruption to be triggered without due cause (or consideration of relevant factors, such as how contained a case is). This particularly benefits those functions (e.g. handling of customers' personal data or submissions) which are better performed on-premise for regulatory compliance reasons.

Exhibit 4.1: Adhering to social-distancing guidelines at bank branches

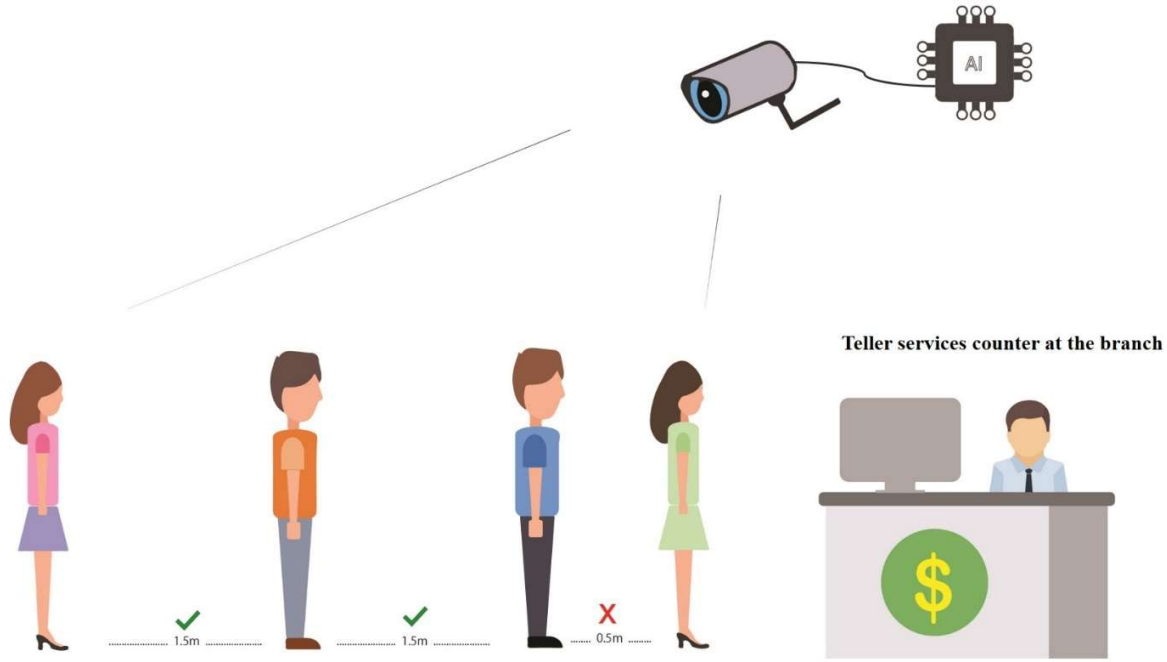
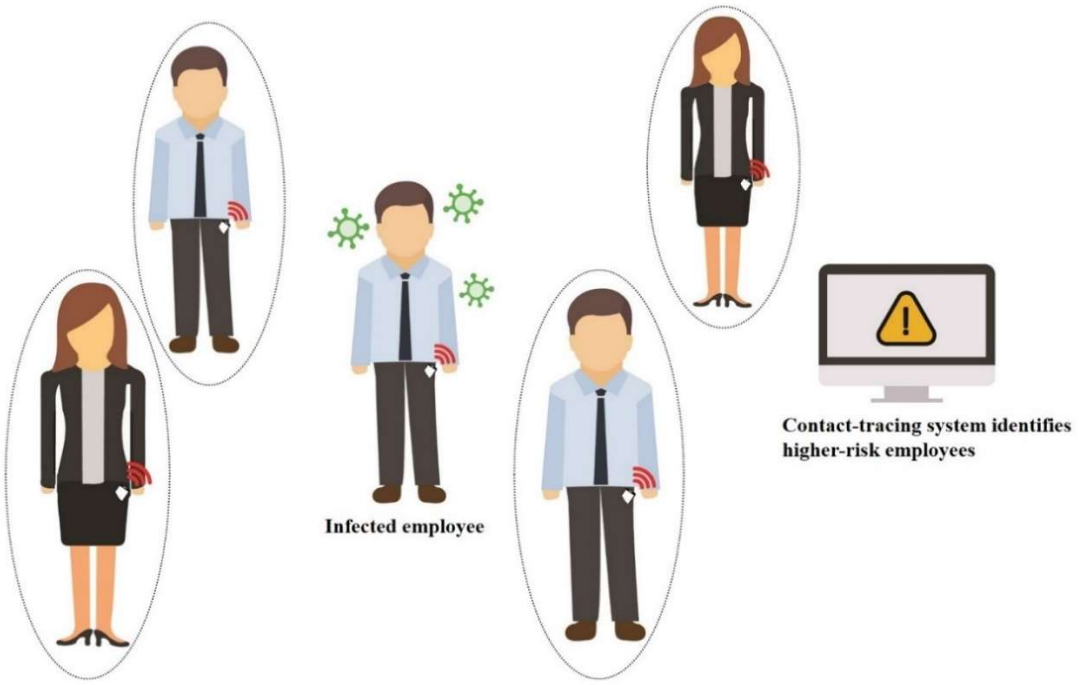


Exhibit 4.2: Identification of employees at higher risk from COVID-19 exposure



The use cases above demonstrate the pivotal role that technology can play in helping the banking industry overcome the difficulties presented by the COVID-19 outbreak. The HKMA encourages the banking industry to closely work with the technology sector to explore relevant Regtech solutions. Appreciation is also extended to those technology firms that have been helping other industries as well as the public ride out the challenges presented by COVID-19, including by offering free or discounted deployment, services, and tools. If not already done, banks should take the catalytic opportunity of COVID-19 to consider and set a strategic direction for their digitalisation journeys.

This newsletter is benefited by input and ideas contributed by the following companies:
- Coöperatieve Rabobank U.A.
- LeapXpert Limited