April 10, 2020
Mizuho Financial Group, Inc.
Mizuho Bank, Ltd.

Mizuho begins proof-of-concept trial of Digital ID based on device location information and facial recognition for use in authentication and ongoing customer due diligence

In May 2020, Mizuho Bank, Ltd. (President & CEO: Koji Fujiwara), a core subsidiary of Mizuho Financial Group, Inc. (President & CEO: Tatsufumi Sakai), will begin a proof-of-concept trial of a new Digital ID in cooperation with Google Cloud Japan G.K.; Nomura Research Institute, Ltd.; and Dai Nippon Printing Co., Ltd. The Digital ID improves online banking authentication and ongoing customer due diligence (CDD) by utilizing device[1] location information (geolocation) and facial recognition technology. The trial will be a first step towards establishing IT system infrastructure for the Digital ID and launching it as a full-fledged service.

This proof-of-concept trial is the sixth project Japan's Financial Services Agency has selected for support under the FinTech Proof-of-Concept Hub initiative.[2]

1. Smartphones, tablets, laptops, and other mobile devices.
2. FinTech Proof-of-Concept Hub: This initiative, run by Japan's Financial Services Agency, facilitates fintech-related proof-of-concept trials in order to accelerate fintech innovation. Through the initiative, Japan's Financial Services Agency provides ongoing support to fintech businesses, banks, and other organizations conducting trials to address relevant practical issues, including identifying any potential risks in terms of compliance or supervision as well as any potential conflicts in terms of the interpretation of the law which may arise when bringing the service to market.

1. Background of the proof-of-concept trial

Cybercrime has been on the rise in recent years, with Japan seeing a record 9,519 confirmed cases in 2019.[3] More widespread use of online banking has also led to an increased threat of crime. Currently, for the sake of balancing security and convenience, online banking authentication mainly relies on two-factor authentication, in which one factor is something the user knows, such as an ID and password, and the other factor is something the user has, such as a dedicated card or a one-time password. However, two-factor authentication cannot completely eliminate phishing-based password theft, unauthorized lending of dedicated cards to others, and similar forms of unauthorized access. Consequently, there is a need to

further enhance security without sacrificing customer convenience.

3. Source: National Police Agency of Japan, “State of Cyber Threats in 2019” [*reiwa gannen ni okeru saibā kūkan wo meguru kyōi no jōsei nado ni tsuite*], March 5, 2020.

There is also a need for financial institutions to strengthen CDD, an important responsibility in combating money laundering and financing of terrorism and one the Financial Action Task Force on Money Laundering (FATF) has made a priority.

Against this backdrop, we are implementing the proof-of-concept trial to evaluate whether or not device location information and facial recognition technology can ensure security in online banking and, in the case of device location information, enhance CDD.

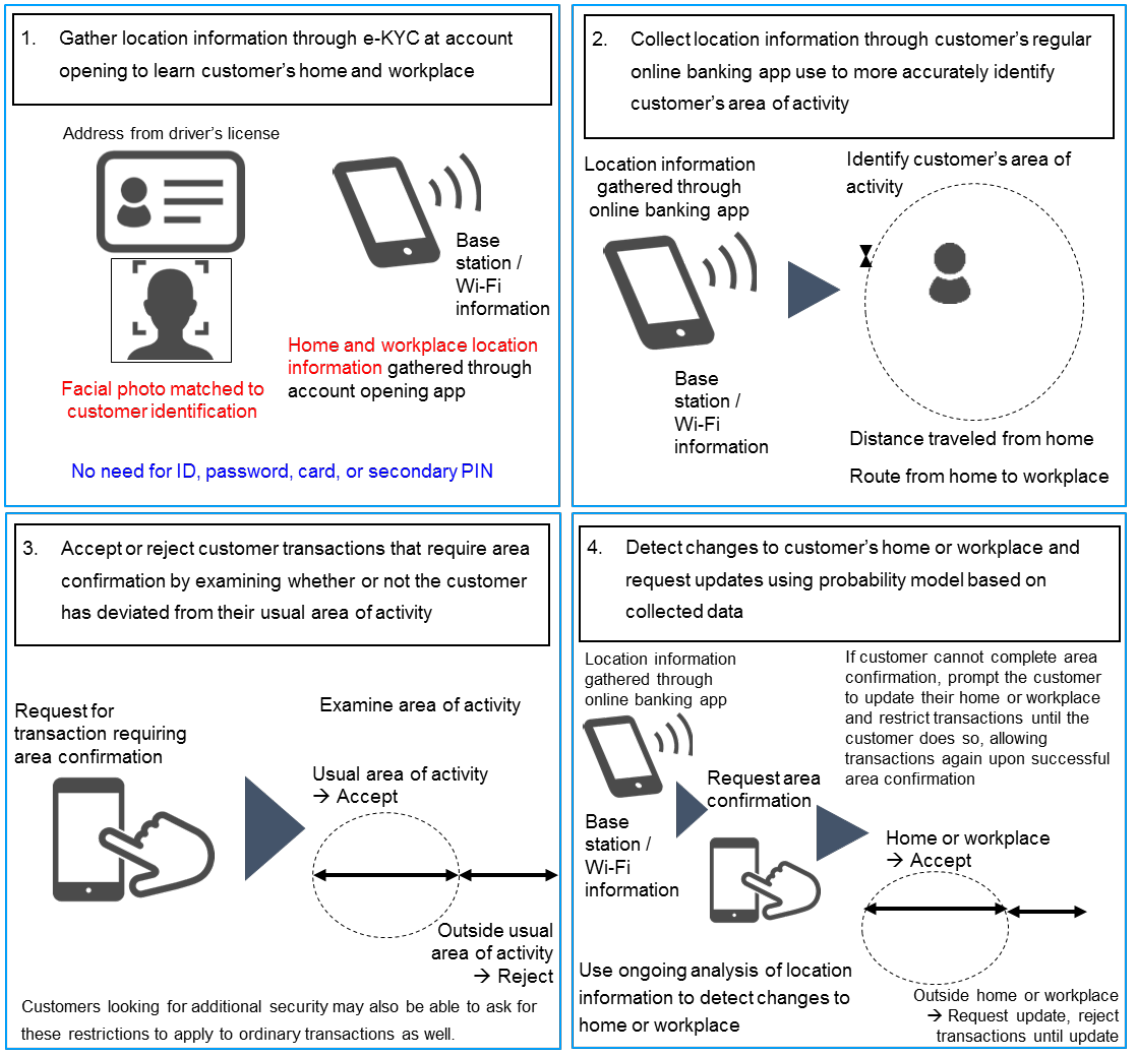
2. Purpose of the proof-of-concept trial

In this proof-of-concept trial, we will test the functions below with the aim of turning them into services and creating new value.

<u>Digital ID based on location information and facial recognition technology</u>

1) Secure authentication based on location information and facial recognition technology
   - Prevent unauthorized access by restricting authentication on devices to near one’s home or other address.
   - Prevent phishing and other forms of fraud by requiring facial recognition.
2) Authentication on any device with cloud syncing
   - Maintain security and convenience even in the event of device loss by combining facial recognition, which is always available, with cloud syncing (allowing for flexible and accurate re-authentication when a device is lost).
   - Ensure authentication is independent of devices and useable even when devices are not available.
3) Specific authentication settings for each level of service
   - Enable users to restrict handling of high-value transactions on devices to only their homes in order to improve security, prevent unauthorized use, and provide a sense of safety in such transactions.
4) Timely profile updates to reflect changes to addresses and other information
   - Prompt users to update their profiles when their registered information does not reflect actual usage.

Potential uses



3. Proof-of-concept trial outline

1) Test use of a Digital ID based on device location information and facial recognition technology as an alternative for fixed IDs and passwords in online banking authentication.
2) Test effectiveness of the Digital ID based on device location information and facial recognition technology in enhancing CDD.

Trial term: May 11 to October 9, 2020

Trial details:

Use virtual accounts to test account opening (initial registration), fund transfers, address changes, and profile update requests.

Participants and roles:

Mizuho Bank, Ltd.: Design trial, verify results, etc.

Google Cloud Japan G.K.: Provide technical support.

Nomura Research Institute, Ltd.: Develop online banking app and build server system.

Dai Nippon Printing Co., Ltd.: Provide facial recognition technology-based authentication functions, develop API-linked facial recognition functions and e-KYC functions.

Handling of personal information:

We will handle the personal information of proof-of-concept trial participants in conformance with the FISC Security Guidelines.[4]

4. FISC Security Guidelines: The FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions published by the Center for Financial Industry Information Systems of Japan.

4. Initiatives going forward

The results of this proof-of-concept trial will be publicized on the Japanese Financial Services Agency's Fintech Proof-of-Concept Hub website. With commercialization as our goal, we will address not only technical issues but also legal and security issues and thoroughly examine the feasibility of commercializing the service.