FAQ: Touch ID

for Mobile and Tablet Banking Apps

Mobile Banking Apps 4.5

What is Touch ID?

Touch ID is a simple, secure way for end users to access the Apple devices described below using built-in, fingerprint-sensor technology. Digital Insight has leveraged this technology to facilitate the end-user login process to your Mobile Banking Apps in lieu of traditional login credentials.

Is any additional hardware required to enable Touch ID?

No additional hardware is required to enable Touch ID on Touch ID-capable devices.

How do end users enable Touch ID in Mobile Banking Apps?

Upon successful logon into their Mobile Banking App with their username and password on a Touch ID-supported iPhone, end users will receive a prompt asking them if they would like to start using Touch ID to log in.

- If accepted, the end user will be able to log in with Touch ID the next time the Mobile Banking App is opened. The end user also will be prompted to verify their fingerprint for additional security.
- If not accepted, the end user will be prompted one more time after 30 days. After the 30-day period, if the end user wants to enable Touch ID, it can be enabled from the Settings menu in the Mobile Banking App.

Upon successful logon into their Mobile Banking App with their username and password on a Touch ID-supported iPhone, end users will receive a prompt asking them if they would like to start using Touch ID to log in.

When will Touch ID be supported on Tablet Banking Apps/iPads?

Touch ID support for Tablet Banking Apps will be made available on relevant iPads as part of Digital Insight’s Q3 2015 release.

Can end users log in with their username and password if they have enabled Touch ID?

Yes, they can. Digital Insight believes in allowing your users the freedom to choose how they log into your Mobile Banking App.

What are the limitations of Touch ID that my organization should be aware of when deciding whether or not we want to enable it?

There are a few key limitations that your organization should be aware of when deciding whether or not to enable Touch ID:

- Mobile Banking Apps cannot discern between the fingerprints of individuals who are enrolled on the device. Digital Insight is only informed whether or not the fingerprint is valid, which means that it was successfully added to the device's fingerprint repository, and not whether that fingerprint belongs to the owner of a certain username. End users are informed of this limitation directly within the Mobile Banking App. The security model is based on the assumption that the device's owner trusts all individuals who access their device through Touch ID.
- If the end user has multiple unique logins with your organization, Touch ID can only be used with a single login per device.
- End users who log in with Touch ID will have the same level of access to the app as if they had entered a valid username and password.

Is Touch ID compliant with FFIEC cybersecurity guidelines for digital banking?

The FFIEC guidelines recommend multi-factor authentication. With Digital Insight, two-factor authentication is required in order to use biometric authentication. Biometric authentication requires configuration, and during that configuration process, there are at least two factors being setup – what you have, your device where your biometric registration is being configured; and who you are, the biometric data that represents you. In reality, when you swipe your finger or scan your eye, the user is providing these two factors, who they are and what they have. It is important to note that the biometric authentication only works on the device you registered. You cannot go onto another device and use your biometrics unless you have set them up on that device as well.

What testing has Digital Insight completed involving Touch ID and Mobile Banking Apps to ensure the security of the authentication process?

Touch ID is an Apple feature and the reputation of Apple along with the risk it has accepted with this security feature weighed heavily on this decision. In addition, the Touch ID feature has been reviewed and tested according to Digital Insight's Secure Development Life Cycle (SDL/SDLC) process, which includes an architecture review, static code analysis, and manual and dynamic vulnerability testing.

What is Digital Insight's position when it comes to whether or not my organization should enable Touch ID in Mobile Banking Apps?

Digital Insight has no position on this matter. It is up to your organization to make its own determination and balance the benefits and risks before deciding whether or not to enable Touch ID in Mobile Banking Apps.

Can Digital Insight provide recommended verbiage to include in our Terms and Conditions?

Digital Insight does not provide this information. It is up to your financial institution to determine how you would like to communicate the Terms and Conditions with your end users.

Where is the fingerprint information stored? Does Digital Insight have access to it?

Touch ID fingerprints are stored on the device and never leave it. Furthermore, they are encrypted with a key that is only accessible to the device. Mobile Banking Apps cannot access the actual fingerprint. They can only determine if the fingerprint is valid or not.

How has Digital Insight added security to this process?

Digital Insight has strengthened security by:

- Only allowing end users who have gone through the USP migration flow and/or created their account after your organization was migrated onto our Digital Banking Platform. This was done to ensure that each Mobile Banking App enabled for Touch ID has a consumer key created through a secondary authentication flow (MFA).
- Not storing usernames and passwords on the device to support Touch ID. Instead, a token is stored securely in the device's Keychain that cannot be transferred to another device. Digital Insight can invalidate this token on the server, while keeping the username and password combination safe.
- If a user tries to log in using Touch ID, but cannot provide a valid fingerprint after five tries, they must enter their device passcode to re-enable Touch ID.

Can end users still log in if they are on hold or need a password reset?

If an end user's account is on hold, they cannot log in. However, even if the account requires the password to be reset, Touch ID still can be used to log in. Touch ID is an alternative credential for end users.

Are there any new reports around Touch ID (new audit logs)?

Yes, we added new data points to the audit logs to determine when end users have enabled Touch ID and when they have logged in with it.

How can an end user disable Touch ID in Mobile Banking Apps?

There are two ways:

• Disable Touch ID in the Settings menu of the Mobile Banking App.

• Un-enroll all fingerprints or disable the device passcode from the device's Settings menu.

NOTE: Re-enabling Touch ID from the device Settings will also re-enable it for Mobile Banking Apps if users have not disabled it in the app settings.

What happens if a Touch ID-enabled device is stolen?

First, instruct your end user to log into iCloud (https://www.icloud.com/) and remotely wipe their device.

• After logging into iCloud, end users should start the "Find My iPhone" app, select the device/s they have lost and erase the data on the device/s.

Next, contact Digital Insight customer support and request them to invalidate the token on the Digital Insight side. Further improvements are planned to make this feature available through the Admin Platform. The timing on the release of this feature is still to be determined.