Introducing Biometric Security for the Hearsay Social Mobile App

We're excited to announce that the Hearsay Social Mobile App now supports Biometric Security. This increases protection at the application level for your company and client data.

This additional layer of security doesn't require device management, and it enables protection on both managed and unmanaged devices to support all mobility models (BYOD, CYOD and COPE). End-user productivity won't be affected by this increased security.

To unlock the application for a user, the Hearsay Social application will use the mobile device's preferred security method—either facial recognition or fingerprint—to provide access to secure conversations almost instantaneously.

Advisors can be confident that sensitive data within the application is protected behind an additional wall of security if their device is compromised (for example, if a child should find the phone and start posting).

Compliance and IT leaders benefit from knowing that many potential end-user vulnerabilities are being mitigated and that by using Hearsay, they are following guidance provided in FINRA's 2018 Report on Selected Cybersecurity Practices.

FAQs

Q: Can Biometric Security be configured by my Hearsay admin?

A: No, it must be configured by the Hearsay team. Clients should contact their CSM regarding enablement.

Q: Can this be set by hierarchy?

A: No. Biometric Security can only be set organization-wide.

Q: Where is a user's biometric data stored? How are we ensuring compliance with biometric security laws?

A: Biometric data is stored on the user's own device; not by Hearsay Social. The device validates whether or not the biometric scan matches what it has recorded (whether it's fingerprint or FaceID). If the scan matches, the application unlocks; if it doesn't match, the application does not unlock. If the biometric unlocking fails the maximum number of times (3 times on iOS; 5 times on Android), the user will need to log in to Hearsay Social via email.

How Biometric Security Works

1. If an organization enables Biometric security, each user will be asked to set it up on their device. The next time each user launches the Hearsay Social mobile application, they will follow the process outlined below for their type of device:

    a. iOS – The user will need to grant permission for FaceID or TouchID (depending on their device model).
    b. Android – If the user has already set up and enabled fingerprint scanning on their device, the Social application will use this as an unlocking method.

2. When an inactivity timeout occurs, the user opens the Social application and is prompted to unlock the application using the biometric method available on their device (iOS/FaceID, iOS/Touch ID, Android/Fingerprint):

    a. The user does this via their phone's version of Biometric Security (this will be fingerprint or FaceID depending on the device).
    b. If the phone does not have biometric capabilities (older Android devices, for example), PIN or pattern will be used to unlock the Hearsay Social application.

3. When the mobile login session expires (this is configured for each organization), the user will have to log in via email.

Find out how Hearsay can help your advisors and agents, contact us at:

VISIT   hearsaysystems.com

EMAIL   contact@hearsaysystems.com

CALL   +1 415-692-6230
               +1 888-990-3777

ABOUT HEARSAY SYSTEMS

Hearsay Systems is reinventing the client experience in Wealth Management, Insurance and P&C with compliant digital communications and workflow solutions. Over 150,000 advisors and agents at the world's largest financial services and insurance firms leverage Hearsay to engage with customers and build stronger relationships to grow their business.

With Hearsay Cloud for financial services, advisors and agents provide real-time, personalized and seamless client experiences across the right channel - social, texting and mobile - at the right moment. Automated, pre-built industry workflows for insurance and wealth management provide one-click actionable suggestions for targeted engagement. Built for the enterprise, Hearsay Systems connects data and every client interaction to corporate CRM systems and digital marketing programs – all on a secure, compliant enterprise-ready platform.

Hearsay is headquartered in Silicon Valley with locations throughout North America, Europe and Asia. Connect on Facebook, Twitter, LinkedIn and the Hearsay blog.