Biometric Data Privacy Policy for the Chase Biometrics Product

Effective: March 1, 2026

Purpose

This Policy and Notice explains how JPMorgan Chase Bank, N.A. ("we," "us", "our" or "JPMC") and our vendors collect, use, store, transmit, disclose, protect, retain, and destroy biometric data with respect to the Chase Biometrics product, and the purposes for which biometric data is processed.

This policy covers how we collect, use, disclose, and retain your biometric data only. Other personal information is covered by our applicable privacy policies available here.

Definition of "Biometric Data"

"Biometric Data" means any of your personal biological characteristics or measurements, or information based on or derived from such a characteristic or measurements, that can be used to identify or authenticate you, and as may be defined in other applicable local laws that govern the collection, use, processing, storage, sharing, or disclosure of biometric data. Biometric Data includes mathematical template created from the physical characteristics of your face, retina or iris scan, fingerprint, voiceprint, or hand or palm geometry used to identify or authenticate you as an individual.

Collection and Use of Biometric Data

We and/or our vendors will collect, store, use, and/or transmit your Biometric Data solely for:

- Identity authentication;
- Security;
- Fraud prevention;
- Improving the Chase Biometrics product; and
- Dispute management and resolution.

If you decline to provide Biometric Data at enrollment or checkout, you will need to complete your purchase using an alternative payment method.

Disclosure of Biometric Data

We will not disclose your Biometric Data to any person or entity other than our vendors, unless:

- You provide express consent;
- Disclosure is required by applicable law;
- Disclosure is required pursuant to a valid regulatory or governmental request, court order, warrant, or subpoena; or
- In connection with corporate changes (that is, in the event of a merger, acquisition, or sale of all or any relevant portion of our business or assets).

Security Safeguards

We and our vendors will use reasonable care and appropriate administrative, technical, and physical safeguards to store, transmit, and protect any paper or electronic Biometric Data from loss or unauthorized access, use, or disclosure. We protect Biometric Data at least as strongly as other highly sensitive personal information we handle, including government-issued identification and financial

account data. For more information on data security at JPMC, please visit: https://www.chase.com/digital/resources/privacy-security

Retention of your Biometric Data

When we or our vendors retain Biometric Data, it will be destroyed within one of the following timeframes, whichever occurs first:

- Within one year of the date on which the initial purposes for collecting the data have been satisfied;
- Within three years from the date of your last use of Chase Biometrics; or
- When required by law.

No Sale or Profit from Biometric Data

We and our vendors do not sell, lease, trade, or otherwise profit from Biometric Data.

Rights and Contact Information

You may have rights regarding Biometric Data (e.g., access, deletion, or withdrawal of consent where permitted). To exercise available rights or to ask questions, contact 1-800-517-8197.

Changes to This Policy

We may update this Policy to reflect changes in technology, practices, or legal requirements. Material changes will be communicated through appropriate channels and, where required, consent will be obtained.

Contact us

You can reach JPMorgan Payments at 1-800-517-8197.