convera
SMART MONEY MOVES

Biometric Information Privacy Policy

Last updated: August 17, 2026

Convera ("**Convera**", "**we**," "**us**," or "**our**") has adopted this Biometric Information Privacy Policy ("**Biometric Policy**") to explain how biometric identifiers and biometric information (together, "biometric data") are handled in connection with certain identity verification and fraud-prevention checks that may be subject to the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq. ("BIPA").

This Biometric Policy supplements the Convera Global Privacy Notice (available at: https://convera.com/privacy/) and applies only to the processing of biometric identifiers and biometric information covered by BIPA in the context described below. If there is any conflict between this Biometric Policy and the Convera Global Privacy Notice regarding biometric identifiers or biometric information subject to BIPA, this Biometric Policy governs and controls over any general descriptions of personal data processing in the Convera Global Privacy Notice.

This Biometric Policy is intended to address Convera's obligations under the Illinois Biometric Information Privacy Act (740 ILCS 14/1 et seq.). Other biometric and privacy laws may also apply depending on the individual's location and the context of processing. Where applicable, Convera addresses those requirements through a combination of this Biometric Policy, the Convera Global Privacy Notice, and any jurisdiction-specific notices, disclosures, or consent mechanisms presented in the relevant workflow.

Who "you" are. Depending on the context, "you" or "your" may include a representative or other relevant individual (for example, a signatory, director, ultimate beneficial owner, or authorized user) associated with a business entity that Convera serves.

What is "biometric data"?

As used in this Policy, biometric data includes "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq.

"**Biometric identifier**" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include (among other things) photographs and certain other excluded categories.

"**Biometric information**" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

When and how biometric data is collected/obtained

We use a third-party identity verification service provider, **Onfido Ltd. (an Entrust Company)**, in certain onboarding and re-accreditation workflows to verify identity (e.g., match a face to an identity document) and to perform certain checks, such as assessing the authenticity of images, videos, and identity documents, including detecting whether there is a genuine human or physical document in the submitted materials, detecting signs of tampering, and detecting and preventing fraud, including signs of coercion or social engineering.

What you may provide in the workflow. Depending on the specific check(s), you may be asked to provide:

- a selfie photo and/or selfie video (and potentially audio), and
- images of identity documents, captured via your device camera or uploaded.

What Onfido does. Onfido processes these inputs and may create or analyze biometric identifiers (for example, a facial geometry scan and/or voiceprint) and associated biometric information to provide a verification or fraud prevention outcome.

Roles. For BIPA purposes, Convera may "collect, capture, or otherwise obtain" biometric data through this workflow (even where Onfido performs the scanning or processing as Convera's service provider).

What Convera stores vs. what Onfido stores

Onfido stores and deletes biometric data (such as any facial geometry scan/template and/or voiceprint) as our service provider, following Convera's instructions and Onfido's documented policies available at: https://www.entrust.com/legal-compliance/data-privacy.

Convera does not store biometric identifiers or biometric information (for example, Convera does not store facial geometry templates or voiceprints).

Convera may receive the verification result and may separately retain certain non-biometric records (such as identity document images and selfies or videos) for legal, regulatory, and financial crime compliance purposes (e.g., KYB/KYC/AML documentation), as described in the Global Privacy Notice. Convera does not use the non-biometric records it retains to create biometric identifiers or biometric information, nor does it run facial recognition on those retained images or videos for unrelated purposes. If that changes, Convera will provide additional notice and obtain any required consent.

Purpose of processing biometric data

Biometric data processed by Onfido on our behalf is used only to:

- verify identity (including matching a face to an identity document);
- authenticate the use of our services (where applicable);
- evaluate the authenticity of your information;
- detect and prevent fraud; and
- help Convera meet and demonstrate our legal obligations, including KYB/KYC/AML and related compliance obligations.

Convera does not use biometric data for marketing or advertising purposes, or for profiling unrelated to compliance or fraud prevention.

Notice and consent ("written release")

Before Convera or its service providers collect, capture, or otherwise obtain biometric data subject to BIPA, Convera will:

- inform you in writing that biometric data is being collected or stored;
- inform you in writing of the specific purpose and the length of time for which biometric data is being collected, stored, and used; and
- obtain your written release (which may be provided electronically) or that of your legally authorized representative.

Retention schedule and permanent destruction

BIPA requires a public written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose is satisfied or within three years of your last interaction with the private entity, whichever occurs first, absent a valid warrant or subpoena.

Convera's retention and destruction approach for biometric data in this workflow is set out as follows:

- **Biometric identifiers and information** (e.g., facial geometry scans/templates, voiceprints): Convera instructs Onfido to permanently delete biometric data within sixty days from session initiation (or sooner where feasible), and in any event no later than when the initial purpose is satisfied or within three years of your last interaction with Convera (whichever occurs first), unless retention is required by a valid warrant or subpoena issued by a court of competent jurisdiction. For this purpose, "session initiation" means the date and time when the individual first starts the identity verification workflow in the Onfido environment, whether or not the workflow is completed.
- **Non-biometric records retained by Convera** (e.g., document images/selfies/videos retained for legal, compliance and regulatory documentation): retained in accordance with our Global Privacy Notice and applicable financial services/AML recordkeeping requirements. These records are not retained as biometric identifiers or biometric information.

Disclosure of biometric data

Convera and Onfido will not disclose, redisclose, or otherwise disseminate biometric identifiers or biometric information except as permitted by BIPA, including:

- with your consent;
- to complete a financial transaction you requested or authorized;
- where required by law or ordinance; or
- pursuant to a valid warrant or subpoena from a court of competent jurisdiction.

Convera does not disclose biometric data for commercial marketing purposes.

No sale or profit

Neither Convera nor Onfido sells, leases, trades, or otherwise profits from biometric identifiers or biometric information.

Security Safeguards

BIPA requires entities in possession of biometric identifiers or biometric information to store, transmit, and protect such data using a reasonable standard of care within the industry and in a manner that is the same as or more protective than other confidential and sensitive information.

Consistent with this requirement, Convera requires appropriate safeguards, including (as applicable) encryption in transit and at rest, access controls and least-privilege principles, logging and monitoring, vendor security requirements, and secure deletion procedures. Onfido is contractually required to maintain reasonable and appropriate technical and organizational safeguards consistent with BIPA's standards.

Biometric processing outside Illinois

Where biometric data is processed in a jurisdiction that treats biometric data as sensitive or special category data, including under the GDPR or UK GDPR where biometric data is processed for the purpose of uniquely identifying an individual, Convera

will process such data only where it has an applicable lawful basis and, where required, a condition for processing sensitive or special category data. This may include explicit consent or another condition permitted by applicable law, such as substantial public interest where supported by applicable law and appropriate safeguards.

Changes to this Biometric Policy

We may update this Biometric Policy from time to time. We will revise the “Last updated” date when we do.

Contact Us

Questions related to this Biometric Policy may be sent to privacymatters@convera.com or via the contact information in the Convera Legal Entities appendix, c/o Privacy Office, in our Global Privacy Notice.