Biometric Information Privacy Policy

B9 has adopted the following biometric information privacy policy:

Definitions

“Biometric Data”, including biometric identifiers and biometric information, means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, regardless of how it is captured, converted, stored, or shared, which is used to identify an individual.

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

“Know Your Customer (KYC)” also known as customer due diligence or know your client, is the process of verifying current or prospective customers’ identities and assessing the potential risks of doing business with them. Digital KYC platforms are usually able to verify users in a variety of ways, from documentary verifications such as government IDs and utility bills to selfies and database verifications from authoritative and issuing sources like the IRS.

"Written release" means informed written consent or, in the context of employment, a release executed by an customer as a condition of employment.

Purpose for Collection of Biometric Data

B9 or its designated vendor shall collect, store, and use biometric data solely for customer identification and fraud prevention purposes.

Disclosure and Authorization

To the extent that B9, or a vendor of B9, captures, or otherwise obtains biometric data relating to a customer, B9 must first:

a. Inform the customer in writing that B9, or its vendor, is collecting, capturing, or otherwise obtaining the customer’s biometric data;

b. Inform the customer in writing of the specific purpose and length of time for which the customer’s biometric data is being collected, stored, and used; and

c. Receive a written release signed by the customer (or his or her legally authorized representative) authorizing B9, or its vendor, to collect, store, and use the customer's biometric data for the specific purposes disclosed by B9, and B9 will not sell, lease, trade, or otherwise profit from customers' biometric data.

Disclosure

B9 will not disclose or disseminate any biometric data to anyone unless:

a. The customer consents to such disclosure or dissemination;

b. Disclosing the data completes a financial transaction requested or authorized by the customer;

c. Disclosure is required by state or federal law or municipal ordinance; or

d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

Unless otherwise required by federal or state regulations, B9 (and its vendor) shall retain customer biometric data only until, and shall permanently destroy such data when, the first of the following occurs:

a. The initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the customer's relationship with B9 and the permanent destruction of associated records has been authorized; or

b. Within 3 years of the customer's last interaction with B9.

Data Storage

B9 shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which B9 stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as account numbers, PINs, driver's license numbers and social security numbers.

Policy

B9 will not disclose or disseminate any biometric data to anyone other than B9's customer onboarding vendor. Customers will be advised that B9 and its onboarding vendor shall collect, retain, and use biometric data for the purpose of identifying customers in conformity with customer identification requirements imposed by federal regulations. B9 or its assigned vendor shall use computer systems to determine facial geometry in customer identifying documents so that unique data points may be used to create a unique mathematical representation in order to verify the customer's identity. Both State and Federal statutes regulate the collection, storage, use, and retention of "biometric identifiers" and "biometric data." The customer will be free to decline to provide biometric identifiers and biometric data to B9 and its vendor; however, declining such permission will prevent B9 from completing KYC of the customer. Any customer that refuses to provide full KYC will be allowed only partial access to B9 membership. Customers may request a copy of this policy at any time.