Job Applicant and Workforce Privacy Notice

Effective Date: January 1, 2023

Trustmark Mutual Holding Company and our subsidiaries ("Trustmark", "company", "we", "our" or "us") developed this Workforce Privacy Notice ("Notice") to provide you with information about how we collect, use, and disclose personal information in the context of working with us and the choices you have with respect to that information.

This Notice applies to job applicants (past and present), employees (current, former, regular, part-time, temporary), non-employee contingent workers, contractors, and consultants (collectively, "workforce member", "you" or "your"). This Notice is not intended to create any express or implied promise or contract for employment nor does it apply to your use of our products as a consumer.

You should be aware that data privacy laws can vary in different jurisdictions where Trustmark operates and where it has employees. Trustmark's policy is to comply with the requirements of all applicable laws and internal policies, including obtaining your consent where required. To the extent this Notice conflicts with applicable law, that law will control.

Personal information we collect

"Personal information" is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with you. Personal information does not include data that has been rendered in such a way that an individual is not or no longer identifiable.

The table below describes the categories of personal collection that we may collect and that we may have collected from workforce members in the previous twelve (12) months.

Category	**Categories of Sources**	**Disclosed for a Business Purpose?**	**Sold or Shared with Third-Party so They Can Market to You**	**Purposes for Which Information is Collected**
Personal identifiers or characteristics. • Such as name, former name, alias, postal address, email address, telephone number, Social Security number, driver's license number, state identification number, passport number, insurance policy number, unique personal identifier, online identifier, Internet Protocol (IP) address, account name, signature, education, employment, employment history, bank account number, credit card number,	• Directly from you. • From other businesses (e.g., benefits providers). • From publicly available sources such as company websites or professional networking sites. • From professional references.	Yes	No	To assess suitability and qualifications of applicants for employment; process employment applications; onboard workforce members; enroll and administer medical and other benefits; verify your identity or the information you provide to us; enter into agreements; comply with applicable income tax, employment, and immigration laws; to protect and take action against malicious, deceptive, fraudulent, illegal actions, or security incidents; and for general human resource management purposes. For employment applications submitted through our website, we may collect your IP address through the use of a cookies or similar technologies to enable the use of the specific service

debit card number, or any other financial information, medical information, or health insurance information.				explicitly requested by you. For more information, please see the privacy policy of the website you visited. For payment purposes such as pay rate, payroll deduction information, and banking information for direct deposit; credit card information for expense reimbursement; and to comply with applicable laws.
Protected classification characteristics. • Such as age, race, ancestry, national origin, citizenship, marital status, pregnancy, medical condition, physical or mental disability, sex, veteran or military status and other protected classifications under state or federal law.	• Directly from you.	Yes	No	For equality and diversity purposes for applicants and workforce members, such as minority, veteran, and disability status, through voluntary self-disclosure and other means to implement Trustmark's diversity programs and to comply with applicable laws. For health and safety purposes to maintain a safe workplace; assess working capacity; administer health and workers' compensation insurance programs; for workforce planning; and to comply with applicable laws. When necessary for benefits enrollment and administration purposes.
Commercial information. • Such as insurance records and license requirements, etc.	• Directly from you.	Yes	No	If you are a contractor, we may collect commercial information from or about you in connection with obtaining services from you.
Biometric information. • Such as fingerprints, iris or retina scans.	• Directly from you.	Yes	No	Fingerprints if required by law and for background check purposes; fingerprints or other biometric information for secure access purposes. Health or exercise data in connection with wellness programs. Trustmark collects this information to ensure that workforce members properly log-in to company equipment and ensure that authorized workforce members have access to secured locations.
Internet or other similar network activity. • Such as browsing history, interactions with features in our IT systems and applications, including your username, IP address, emails and other electronic communications, documents, files, websites accessed, and log files of Trustmark computer system usage ("IT Data").	• Indirectly from you by observing/monitor your actions on our IT systems.	Yes	No	**Storage and processing relating to use of our IT systems.** To provide workforce members with IT resources and support, such as password resets, email capabilities, new user accounts, or troubleshooting; to monitor the correct functioning and ensuring the security of Trustmark IT systems and preventing misuse and outside attacks or threats; to transmit and archive information, such as email messages; to prevent the commission of crimes and other violations of law facilitated by our IT systems; to ensure compliance with software licenses and other agreements; to comply with legal obligations in connection with pending or threatened litigation; to prevent theft

				or unauthorized disclosure of our intellectual property or confidential information; and to assessing compliance with, and detecting potential or actual violations of, Trustmark policies or any applicable laws and regulations. **Investigations.** To investigate, store, review, and disclose any IT Data or information created or modified using our systems that is related to internal or governmental investigation. **Access to emails, files, websites, documents, and Instant Messaging program (IM) sessions.** To ensure the security of our IT systems and other IT resources, and prevent any serious threat to, or violation of, our interests or policies, we reserve the right – but does not assume any obligation – to monitor, access, retrieve, review, intercept, block, distribute, and delete, to the greatest extent permitted by applicable law, any email, IM message, IM transcript, website URL, file or document created, sent, received, accessed or stored on or through Trustmark IT systems.
Sensory data. • Such as audio, electronic, visual, or similar information, including information collected via call recordings, recorded meetings, videos, photographs, and CCTV footage.	• Directly from you.	Yes	No	We use the Personal Information to schedule and conduct virtual interviews. For identification purposes (e.g., photo ID badges); to record training sessions or for business-related meetings in accordance with our policies; for on-site surveillance to prevent and deter crimes, protect public safety, and facilitate official investigations into criminal activities or policy violations; and to feature workforce members in promotional materials and on our websites.
Professional or employment-related information. • Such as workforce member ID number, office contact information, work email, qualifications, licensing, details of grade and job duties, absence records, workforce member evaluations and performance information, business travel data; details of disciplinary or grievance investigations and	• Directly from you. • From publicly available sources such as company websites or professional networking sites. • From professional references.	Yes	No	We use the Personal Information we collect to evaluate your qualifications, suitability, and other relevant characteristics; to review and assess information you provide in connection with your application. To manage our relationship with our workforce members.

proceedings, training records, or other related information.				
Education information. • Such as such as education records, including grades, transcripts, student disciplinary records, or any other information you chose to provide. • Information about education history or background that is not publicly available personally identifiable information as defined in the federal Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).	• Directly from you. • From educational institutions or providers of educational or professional certification information.	Yes	No	We use the Personal Information we collect to evaluate your qualifications, suitability, and other relevant characteristics; to review and assess information you provide in connection with your application. For educational expense reimbursement programs.
Health information.	• Directly from you.	Yes	No	That which you voluntarily provide to us for work-related accommodations, sick leave, workers' compensation, wellness programs, or health insurance. To the extent permitted by law, we may also collect health information through contact tracing or health screenings to protect the health and safety of our workforce members and visitors.
Beneficiary information. Such as name, contact information, relationship to you, birth date, Social Security number.	• Directly from you.	Yes	No	If you voluntarily provide such information for purposes of designating a recipient of your benefits in the event of your death.
Dependent information. Such as name, contact information, and relationship to you.	• Directly from you.	Yes	No	If you voluntarily provide such information for purposes of enrollment and administration of benefits and other human resource purposes that involve such dependents.
Emergency contact information. • Such as name, contact information, and relationship to you.	• Directly from you.	Yes	No	To contact your designated emergency contact person in the event of an emergency.

Additional business purposes for processing personal information

In addition to the purposes described above, we may also use the categories of personal information for the following business purposes (and any directly related purposes):

- **Auditing, reporting corporate governance, and internal operations.** Relating to financial, tax and accounting audits, and audits and assessments of our business operations, security controls, financial controls, or compliance with legal obligations and for other internal business purposes such as administering our records retention program.
- **Mergers and acquisitions and other business transactions.** For purposes of planning, due diligence, and implementation of commercial transactions, such as mergers, acquisitions, asset sales or transfers, bankruptcy or reorganization or other similar business transactions.

- **Defending and protecting rights.** To protect and defend our rights and interests and those of third parties, including to manage and respond to workforce member and other legal disputes, to respond to legal claims or disputes, and to otherwise establish, defend or protect our rights or interests, or the rights, interests, health, or safety of others, including in the context of anticipated or actual litigation with third parties.
- **Compliance with applicable legal obligations.** Relating to compliance with applicable legal obligations (such as hiring eligibility, responding to subpoenas and court orders) as well as assessments, reviews and reporting relating to such legal obligations, including under employment and labor laws and regulations, Social Security and tax laws, environmental regulations, workplace safety laws and regulations, and other applicable laws, regulations, opinions, and guidance.
- **Trustline ethics hotline**. To facilitate the administration of our ethics hotline and provide for internal audits and investigations related to the hotline.

Sharing your personal information

In the previous twelve (12) months we have disclosed the above categories of personal information for a business purpose to the following categories of recipients on a need-to-know basis:

- **Our workforce members**
- **Service providers**. We use service providers to operate, host and facilitate our operations and business (including human resources operations). These include hosting, technology, and communication providers; security and fraud prevention consultants; analytics providers; background and reference check screening services; payment processors, legal services, and hiring process and benefits management and administration tools.
- **Government authorities and law enforcement**. In certain situations, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- **Business transfers**. Your personal information may be transferred to a third party if we undergo a merger, acquisition, bankruptcy. or other transaction in which that third party assumes control of our business (in whole or in part).
- **Professional advisors**. We may share your personal information with our professional advisors.
- **Other**. We may also share your personal information with third parties for purposes of fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting, and investigating security incidents and potentially illegal or prohibited activities; protecting the rights, property, or safety of you, us, or another party; enforcing any agreements with you; responding to claims; and resolving disputes.
- **No sale or sharing.** Trustmark does not sell your personal information to third parties, and we do not allow third parties to use the personal information we provide to them to offer you their products or services.

Retention of personal information

We will retain the categories of personal information we collect for as long as reasonably necessary to support our ongoing legitimate business needs and to carry out the purposes described in this Notice or as otherwise required by law. Generally, this means your personal information will be retained until the end of your employment or work relationship with us plus a reasonable period of time thereafter as required: 1) to effectuate termination of our relationship; 2) by applicable law or regulation; 3) to respond to employment or work-related inquiries; or 4) to provide you with ongoing benefits. If you continue to receive benefits from us after the end of your employment, we will continue to manage and process your personal information as described above.

California Addendum to Workforce Privacy Notice

Scope

This Addendum supplements the Workforce Privacy Notice. It applies solely to the personal information of workforce members, officers, directors and their beneficiaries, dependents, and emergency contacts residing in California (collectively, "California Workforce Members"). In addition to the Notice, this Addendum is intended to satisfy our applicable notice requirements under the California Consumer Privacy Act of 2018 ("CCPA") (Cal Civ. Code § 1798.100 et seq.), as amended by the California Privacy Rights Act ("CPRA"), and its implementing regulations, (hereinafter, "CCPA").

For the purposes of this Addendum, personal information **does not** include:

- Information lawfully made available from government records
- Information made available to the general public by you or widely distributed media
- Deidentified or aggregated information
- Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data; and
- Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994

Use of Sensitive Personal Information

We do not use or disclose workforce member sensitive personal information as defined under the CCPA for purposes except as described in this Notice or as permitted by law. Our collection, use, and disclosure of sensitive personal information is generally limited to what is reasonable and proportionate for the following purposes:

- To perform services or provide products expected by workforce members.
- To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
- To ensure the physical safety of individuals.
- For short-term, transient internal use.
- To perform our functions as an employer.

Privacy Rights

The CCPA provides California Workforce Members with specific rights regarding their personal information as described below. Instructions for making a privacy rights request may be at https://trustmarkbenefits.com/privacy-rights-request. We encourage you to read through this entire section before submitting a request. These rights do not affect other rights you may have under the California Labor Code.

Authorized agents. You may designate someone as an authorized agent to submit privacy rights requests and act on your behalf. Authorized agents will be required to provide proof of their authorization in their first communication with us, and we may also require that the requestor directly verify their identity and the authority of the authorized agent.

Businesses operating as an authorized agent on behalf of a California resident must provide both of the following:

(1) Certificate of good standing with its state of organization; and
(2) A written authorization document, signed by the California resident, containing the California resident's name, address, telephone number, and valid email address, and expressly authorizing the business to act on behalf of the California resident.

Individuals operating as an authorized agent on behalf of a California resident must provide either of the following:

(1) A notarized power of attorney signed and dated by the California resident naming the authorized agent as the California resident's representative; or
(2) A written authorization document, signed by the California resident, containing the California resident's name, address, telephone number, and valid email address, and expressly authorizing the individual to act on behalf of the California resident.

We reserve the right to reject: 1) requests from authorized agents who have not fulfilled the above requirements, or 2) automated CCPA requests where we have reason to believe the security of the requestor's personal information may be at risk.

Right to know and request access. Subject to the exceptions set forth in the CCPA, you have the right to request that we disclose certain information to you about our collection and use of your personal information. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The categories of personal information that we collected;
- The categories of sources from which we collected your personal information;
- Our business or commercial purposes for collecting your personal information;
- The categories of third parties to whom we disclose your personal information; and
- A copy of the specific pieces of your Personal Information we have collected, subject to whether it involves disproportionate effort on our part to obtain these specific pieces of personal information.

Right to request deletion. Subject to exceptions set forth in the CCPA, you have the right to request that we delete personal information we collected from you. Once we receive and confirm your verifiable request, we will delete and direct our service providers to delete your personal information from our records, unless an exception applies. As an alternative to deletion, your information may be de-identified rather than deleted at our option.

Right to request correction. You have the right to request we correct inaccurate personal information. We will make reasonable efforts to correct your personal information upon request, but if we determine such a request would result in false or inaccurate information, we may reject your request.

Non-discrimination rights. You have the right against retaliation or receiving discriminatory treatment for assertion of your rights under the CCPA. We comply with the non-discrimination provisions of the CCPA.

Right to opt-out. You have the right to opt-out of "sales" and "sharing" of your personal information, as those terms are defined under the CCPA. However, we do not sell your personal information to third parties, and we do not allow third parties to use the personal information we provide to them to offer you their products or services so there is no need to exercise these rights.

Right to request limitation of use and disclosure of sensitive personal information. We do not engage in uses or disclosures of sensitive personal information as defined under the CCPA that would trigger the right to limit use of sensitive personal information. Therefore, there is no need to exercise this right.

How to submit a California privacy rights request

California Workforce Members may submit a request to exercise their CCPA rights by using this request form (https://trustmarkbenefits.com/privacy-rights-request) or by contacting us toll-free at 866-816-1727.

Verification process. To protect you and your information, we must reasonably verify that you are the person that is the subject of the request. You will be asked to provide us with your full name, the last four digits of your social security number, your birthdate (day and month), your email address. If the personal information you provide is inadequate based on the sensitivity of the request, we may request additional information from you. The information you provide us for this purpose will not be further processed. If after a good faith attempt, we cannot reasonably verify your identity or the authority under which the request is made, we will not be able to fulfill your request.

Response timing and process. We will confirm receipt of requests within ten (10) business days. We endeavor to respond to a verifiable request within forty-five (45) days of its receipt. If we require more time or additional information to fulfill your request, we will tell you why.

- If we are unable to fulfill your request or if we deny your request in whole or in part, we will provide you with an explanation. We may direct you to our general business practices for collecting personal information.
- Under no circumstances will we provide a requestor with a Social Security number, driver's license number or other government-issued identification number, financial account numbers, any health insurance or medical identification numbers, any account passwords, or any security questions and answers.
- We will use reasonable security measures when transmitting information to a requestor and will deliver data in a readily useable format.
- We are not required to retain any personal information about you that we collected for a single one-time transaction if we do not retain that information in the ordinary course of business. We are also not required to re-identify or otherwise link data that we do not maintain in a manner that would be considered personal information in the ordinary course of business.
- Where permitted under the law, we may charge you a reasonable fee to process your request.

Changes to this Notice

We may change, update, or modify this Notice from time to time. If we make changes to this Notice, we will revise the Effective Date identified at the top of the first page. Any changes will become effective upon our posting of the revised Notice on our websites, intranet, and/or our applicable job application websites.

How to contact us

If you have any questions about this Notice or the ways in which we collect or use your personal information, please contact us at:

Privacy Officer
Privacy Request
Trustmark Companies
PO Box 7961
Lake Forest, IL 60045-7961
Email: privacysecurityoffice@trustmarkbenefits.com