Northern Trust
California Applicant Privacy Notice

This California Applicant Privacy Notice ("**Applicant Notice**") describes our information practices relating to applicants and candidates for employment with The Northern Trust Company and its subsidiaries and affiliates ("**Northern Trust**," "**we**," "**our**," "**us**," or the "**Company**") who are California residents (each an "**Applicant**" or "**you**"). This Applicant Notice is intended to satisfy our notice requirements under the California Consumer Privacy Act 2018, as amended by the California Privacy Rights Act 2020, and its implementing regulations (collectively, the "**CCPA**").

1. Scope and Relation to Other Policies

This Applicant Notice applies to the Personal Information we collect about Applicants who are California residents. This Notice supplements other agreements, including any Non-Disclosure Agreement(s), if applicable.

For purpose of this Applicant Notice, "Personal Information" is any information that identifies, relates to, describes, is reasonably capable of being associated, or could reasonably be linked, directly or indirectly, with you (subject to some exemptions provided under the CCPA). This Applicant Notice does not address or apply to our information practices such as:

- **Business Information**. Company or business information that constitutes trade secrets, proprietary information, intellectual property, Company property, information that includes or affects the rights of others, privileged or investigative materials, or information that helps ensure security and integrity of Company assets.
- **Publicly Available Information**. Information that is lawfully made available from government records, information we have a reasonable basis to believe is lawfully made available to the general public by you or by widely distributed media, or by a person to whom you have disclosed the information and not restricted it to a specific audience.
- **Deidentified Information.** Information that is deidentified in accordance with applicable laws.
- **Aggregated Information**. Information that relates to a group from which individual identities have been removed.
- **Protected Health Information**. Information governed by the Health Insurance Portability and Accountability Act or California Confidentiality of Medical Information Act.
- **Activities Covered by the Fair Credit Reporting Act**. This includes information we receive from consumer reporting agencies that are subject to the FCRA (e.g., information contained in background check reports we obtain as part of our screening process).

This Applicant Notice also does not apply to the Personal Information we collect from Applicants in the context of their personal use of our products and services, which are subject to different notices. For additional information on our general privacy practices, please visit our privacy policy, available at Privacy - North America | Northern Trust.

Our information practices may vary depending upon the circumstances, such as the location or role for which you are applying. Also, in some cases (such as where required by law), we ask for your consent or give you certain choices prior to collecting or using certain Personal Information. We may also provide Applicants additional notices about our information practices that are covered by other laws.

2. Personal Information We Collect

The following identifies the categories of Personal Information we may collect about Applicants (and may have collected in the prior 12 months):

- **Identifiers**. Such as name, alias, maiden or previous names, title, address, telephone number, personal email address, date of birth, unique personal identifier, online identifier, Internet Protocol (IP) address, social security number, driver's license number, passport number, tax identification number, visa details, entitlement to residency, or other similar identifiers.
- **Protected Classifications**. Such as age, race, ancestry, national origin, citizenship, marital status, pregnancy, medical condition, physical or mental disability, sex, veteran or military status and other characteristics of protected classifications under California or federal law. This information is generally collected on a voluntary basis and is used in support of our equal opportunity and diversity and inclusion efforts, as well as any reporting obligations or where otherwise required by law.
- **Professional or Employment-Related Information**. Such as pre-employment information (including criminal history and drug test results), application data, prior employment history, qualifications, licensing, registration, disciplinary record, assessment records, resumes, cover letters, conduct information (including disciplinary and grievance records), and termination data.
- **Education Information**. Such as education records, including grades, transcripts, student disciplinary records, or any other information about education history or background that is not publicly available personally identifiable information you choose to provide.
- **Biometric Information**. Such as fingerprints for screening purposes.
- **Internet or Other Electronic Network Activity Information**. Such as network activity information or usage data including but not limited to browsing history, search history, clickstream data, system logs, user names, passwords, domain, browser type, operating system, as well as interactions with our portals, websites, applications, and platforms, and other network activity information related to your interactions with us.
- **Geolocation Data**. Such as general location data derived from a device.
- **Audio, Electric, Visual, or Similar Information**. Such as audio, electronic, visual, or similar information, including information collected via call recordings, recorded meetings, videos, photographs, and CCTV footage to secure our offices and premises.
- **Inferences**. Such as inferences drawn from any of the information described in this section reflecting your preferences, characteristics, attitudes, behaviors, and abilities.
- **Sensitive Personal Information**. To the extent required by law and/or voluntarily provided by you, we collect information like social security number, driver's license number, state identification card, passport number, fingerprints, racial or ethnic origin, citizenship or immigration status, or union membership, and health information (e.g., as necessary to provide reasonable accommodations).

3. Sources of Personal Information

We generally collect Personal Information identified above from the following categories of sources:

- Directly from you;
- Recruiters and recruiting platforms;
- Employee referrals;

- Publicly available information and sources;
- Former employers;
- Our service providers, representatives and agents;
- Health care providers/professionals (e.g., as necessary to provide reasonable accommodations); and
- References you provide.

4. Purposes for Which Personal Information is Collected

We generally collect, use, and disclose the categories of Personal Information identified above as reasonably necessary for the following business or commercial purposes, as permitted by applicable laws:

- **Recruiting and Hiring**. To review, assess, recruit, consider or otherwise manage Applicants, candidates, and job applications, including: scheduling and conducting interviews; identifying candidates, including by working with external recruiters; reviewing, assessing and verifying information provided, and otherwise screening or evaluating Applicants' qualifications, suitability and relevant characteristics; extending offers, negotiating the terms of offers, and assessing salary and compensation matters; satisfying legal and regulatory obligations; communicating with Applicants regarding their applications and about other similar position(s) for which they may be interested; maintaining Applicant personal information for future consideration; and in support of our equal opportunity employment policy and practices.
- **Security and Monitoring**. To secure our offices, premises, and physical assets, including through the use of electronic access system, and to investigate privacy, security, or workplace-related incidents.
- **Health and Safety**. For health and safety purposes, such as contact tracing or conducting appropriate screenings of Applicants prior to entering or accessing certain locations or premises.
- **Conducting Audits**. To conduct financial, tax and accounting audits, and audits and assessments of Northern Trust's business operations or security and financial controls.
- **Mergers, 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 seek advice from lawyers, auditors and other professional advisers; to establish or defend legal claims and allegations; to protect and defend our rights and interests and those of third parties, including to manage and respond to employee and other legal disputes, to respond to legal claims or disputes, and to otherwise establish, defend or protect our rights or interests, including without limitation, Northern Trust's trade secrets and other intellectual property, and protecting the rights, property, and reputation of Northern Trust and its workforce, or the rights, interests, health or safety of others, including in the context of anticipated or actual litigation with third parties.
- **Compliance with Legal and Regulatory Obligations.** Related to our compliance with applicable legal obligations (such as determining hiring eligibility or responding to subpoenas and court orders) as well as assessments, reviews and reporting relating to such legal obligations and requests (including investigations) from regulators and self-regulatory organizations, including under employment and labor laws and regulations, Social Security and tax laws, environmental regulations, workplace safety laws and

regulations, banking and securities laws and regulations, rules of applicable self-regulatory organizations, and other applicable laws, regulations, opinions and guidance.

Notwithstanding the purposes described above, we do not collect, use, or disclose "sensitive personal information" beyond the purposes authorized by applicable law. Accordingly, we only use and disclose sensitive personal information as reasonably necessary and proportionate: (i) to perform our services requested by you; (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents; (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct; (iv) to verify or maintain the quality and safety of our services; (v) for compliance with our legal obligations; (vi) to our service providers who perform services on our behalf; and (vii) for purposes other than inferring characteristics about you.

5. How We May Disclose Personal Information

Purposes for Disclosing Personal Information

We may disclose the categories of Personal Information we collect for the purposes described above and for the following business purposes:

- **Evaluate Candidacy**. We may disclose Personal Information when it is necessary to provide services you request and where it is necessary to identify Applicants, schedule interviews, and otherwise evaluate your qualifications and eligibility for employment.
- **Compliance and Legal Obligations**. If required to do so by law or subpoena, or if we reasonably believe such action is necessary to comply with the law, judicial proceeding, court order, or the reasonable requests of regulators, law enforcement or other public authorities. We also may disclose personal information to establish or defend legal claims and allegations against us or to protect and defend our rights and interests and those of third parties.
- **Protection of Us and Others**. We may disclose Personal Information if required to do so by law, to protect rights, property, or safety of our other Employees and contractors, our shareholders, clients, prospects, business associates, and guests, ourselves or others; or where we have a legitimate interest in doing so.
- **Corporate Transactions**. As we continue to develop our business, we may buy, merge, or partner with other companies, or obtain or extend financings, and we may disclose Personal Information as part of those transactions (including in contemplation of such transactions, e.g., due diligence).
- **Other Disclosures**. We may disclose Personal Information to others and in ways not described above that we notify you of or that we obtain your consent for.

Categories of Recipients

We may disclose Personal Information to the following categories of recipients:

- **Affiliates and Subsidiaries**. We may disclose your Personal Information with our affiliates and subsidiaries.
- **Business Partners.** We may also disclose your Personal Information to business partners where it is necessary to administer the working relationship, conduct our business, or for business operations purposes.
- **Service Providers**. We may disclose Personal Information to our service providers who perform services on our behalf. Our service providers are required to take appropriate

security measures to protect your Personal Information in line with our policies and are not permitted to use Personal Information for their own purposes.

- **Acquirers of Business Assets**. If we are or may be acquired by, merged with, or invested in by another company, or if any of our assets are or may be transferred to another company, whether as part of a bankruptcy or insolvency proceeding or otherwise, we may disclose or transfer the personal information we have collected from you with or to the other company. We may also disclose Personal Information as necessary prior to completing such a transaction to lenders, auditors, and advisors.
- **Regulatory and Government Entities**. To comply with our legal obligations and where otherwise required by law, we may disclose Personal Information to applicable regulatory and government entities and applicable self-regulatory organizations.
- **Data Analytics Providers**. To undertake internal research and recruit you for a position with us, we may disclose the following categories of Personal Information to data analytics providers: identifiers and internet and network activity information.
- **Internet Providers, Operating Systems, and Platforms**. If you sign in to or access Company platforms in connection with your application, we may disclose the following categories of Personal Information to Internet service providers, operating, systems and platforms for security and integrity purposes: identifiers and Internet and network activity information.
- **Other Parties with Your Consent**. Personal Information may also be disclosed to others at your request and with your consent.

6. Retention of Personal Information

We store your Personal Information for as long as needed, or permitted, based on the reason we obtained it (consistent with applicable law), and to comply with Northern Trust's record retention requirements. When deciding how long to keep your Personal Information, we consider whether we are subject to any legal obligations (e.g., any laws that require us to keep records for a certain period of time before we can delete them) or whether we have taken any legal positions that require data retention (e.g., issued any legal holds or otherwise need to preserve data). From time to time, we may also deidentify your Personal Information, retain it and use it for a business purpose in compliance with CCPA.

7. Your California Privacy Rights

Applicant Privacy Rights

If you are a resident of California, you may have additional rights regarding your Personal Information under the CCPA. These rights include:

Right to Know/Access. You have the right to request (subject to certain exemptions):

- The categories of Personal Information we collected about you;
- The sources from which we have collected that Personal Information;
- Our business or commercial purpose for collecting, selling, or sharing that Personal Information;
- The categories of third parties to whom we have disclosed that Personal Information; and
- A copy of the specific pieces of Personal Information we have collected.

Right to Correct. Subject to certain exceptions, you have the right to request that we correct inaccuracies in your Personal Information.

Right to Delete. Subject to certain exceptions, you have the right to request deletion of Personal Information we have collected from you. Please note, Northern Trust is not obligated to delete Personal Information that it is required to maintain to comply with applicable laws.

Right to Opt-Out. We do not "sell" or "share" Personal Information (as those terms are defined under the CCPA). We do not sell or share sensitive Personal Information, nor do we sell or share Personal Information about individuals who we know are under sixteen (16) years old.

Right to Limit Use and Disclosure. We do not use or disclose Applicant "sensitive personal information" for purposes except as described in this Applicant Notice (and as permitted pursuant to the CCPA regulations).

Right to Non-Discrimination. We will not discriminate against you for exercising any of the rights described in this section.

Exercising Your CCPA Rights

To exercise any of these CCPA rights, please use one of the following methods:

- **Email**: Privacy_Compliance@ntrs.com
- **Phone**: Human Resources Service Center 1-800-807-0302

Please indicate you are exercising your "CCPA privacy rights." Northern Trust will confirm your identity before fulfilling the request. In some cases, we may request additional information in order to verify your identity, or where necessary to process your request. If we are unable to verify your identity after a good faith attempt, we may deny the request and, if so, will explain the basis for the denial.

You may designate someone as an authorized agent to submit requests and act on your behalf. To do so, you must provide us with written permission to allow the authorized agent to act on your behalf. We may also ask you directly to verify that you have authorized your authorized agent to act on your behalf.

8. Contact Us

If you have any questions or concerns regarding this Applicant Notice or the handling of your Personal Information, please contact us at:

Privacy_Compliance@ntrs.com
Human Resources Service Center 1-800-807-0302

Effective Date: January 1, 2023
Last Updated: November 27, 2023