

Greenleaf Trust (“Greenleaf”) is a privately held wealth management firm with specialized disciplines in wealth management, trust administration, and retirement plan administration. Greenleaf is proud to offer Plan Sponsor and Participants our Fraud Restoration Program (“Program”) in connection with your [for example, Master Services Agreement] [or] [Retirement Plan Service Provider Agreement and Fee Disclosure] (“Agreement”). For accounts where Greenleaf serves as the plan recordkeeper, Greenleaf may restore losses to a Participant’s Greenleaf retirement accounts that result from others’ fraudulent use of Personal Information caused through no fault of Participant.

A. Information Security. Greenleaf seeks to protect the integrity, security, and confidentiality of the information of Plan Sponsor and Plan Participants (“Participants”) and to prevent fraud in connection with Greenleaf providing the services under the Agreement (“Services”).

- i. Personal Information.** “Personal Information” means information provided by or on behalf of Plan Sponsor or Participants, or their agents to Greenleaf in the course of Greenleaf’s performance of the Services under this Agreement that: (i) identifies an individual (by name, signature, address, telephone number or other unique identifier), or (ii) can be used to identify or authenticate an individual.

Personal Information includes (i) an individual’s government-issued identification number (including social security number, driver’s license number, or state-issued identification number); and (ii) financial account number in combination with any required security code, access code, personal identification number, or password, that would permit access to an individual’s financial account.

- ii. Confidentiality.** Greenleaf agrees to keep all Personal Information confidential, using an appropriate degree of care to avoid unauthorized use and disclosure. Greenleaf may disclose Personal Information in accordance with the terms of the Agreement, and additionally to its employees having a need to know this information in connection with the performance of the Services for Plan Sponsor. Greenleaf may also disclose Personal Information to its affiliates and its subcontractors having a need to know this information in connection with the performance of Services. If Greenleaf receives a request for the production of Personal Information under applicable law, Greenleaf shall notify Plan Sponsor in writing before producing any information or documents (except to the extent otherwise prohibited by applicable law).

- iii. Greenleaf Information Security Program.** Greenleaf states that (i) its treatment of Personal Information is in compliance with applicable laws and regulations with respect to privacy and data security, and (ii) it has implemented and currently maintains a written information security program including administrative, technical, and physical safeguards and other security measures necessary (iii) to ensure the security and confidentiality of Personal Information; (iv) to protect against unauthorized access to or acquisition of Personal Information that would likely result in harm to Plan Sponsor or Participant (“Cybersecurity Event”).

As part of Greenleaf’s Information Security Program, (v) Greenleaf maintains at its sole expense cyber-liability insurance coverage subject to certain deductibles, exclusions, and other limitations. Coverage limits may be increased or decreased without notice to Plan Sponsor. (vi) Greenleaf maintains a written Information Security Policy which may be audited by government (for example, Michigan Department of Insurance and Financial Services) or other qualified third-party auditors from time to time. (vii) Greenleaf requires routine cybersecurity training to be completed by all its employees. (viii) Greenleaf shall notify Plan Sponsor, without unreasonable delay, upon

confirming that a Cybersecurity Event has occurred. (ix) Greenleaf shall dispose of all records, electronic or otherwise, including any Personal Information related to Plan Sponsor and its Participants at the completion of the engagement or at Plan Sponsor's request or as required by law.

B. Fraud Prevention and Restoration. For accounts where Greenleaf serves as the plan recordkeeper, Greenleaf will restore losses to a Participant's Greenleaf retirement accounts that result from others' fraudulent use of Personal Information caused through no fault of Participant, provided the following conditions are met subject to the limitations set forth below. Participant accounts may not be reimbursed if these requirements have not been followed. Greenleaf's Fraud Restoration program terms and conditions are available on Greenleaf's website. **Greenleaf will determine the amount of the reimbursement, in its sole discretion, based on the facts of the situation.**

Greenleaf and Plan Sponsor will use commercially reasonable efforts to prevent fraud and unauthorized transactions. The parties agree to the following fraud prevention duties.

i. Greenleaf's Duties

- a. Greenleaf will follow and maintain the Information Security Program described herein.
- b. Greenleaf will verify the identity of Participant before account information may be discussed, before Participant can obtain online account access, and before Participant may obtain a fund withdrawal.
- c. Greenleaf will abide by its Participant Security Protocol, which may be updated from time to time.

ii. Plan Sponsor's Duties

- a. Plan Sponsor will provide all Participants an electronic communication directing them to this Fraud Restoration Program and its terms and conditions, including but not limited to Participant's Duties set forth below within fourteen (14) days of execution of the Agreement.
- b. Greenleaf's Fraud Restoration terms and conditions are available on the Greenleaf Fraud Restoration webpage and may be updated from time to time.
- c. Plan Sponsor will supply Greenleaf with updated Participant records immediately upon change in Participant status.
- d. Plan Sponsor will immediately inform Greenleaf of any cybersecurity events effecting Plan Sponsor or known Participants (for example, phishing, password compromise, email account compromise, ransomware, or other malware).

iii. Participant's Duties

- a. Plan Sponsor will abide by the Participant Security Protocol, which may be updated from time to time. Participant will remain vigilant for fraud.¹

¹ For resources regarding how to prevent fraud on your retirement accounts, visit United States Securities and Exchange Commission fraud prevention website at <https://www.investor.gov/protect-your-investments/fraud/how-avoid-fraud>.

- b. Participant will report suspicious activity to Greenleaf immediately, but no later than sixty (60) days from the suspected unauthorized transaction.
- c. Participant will not share user ID's, passwords, or challenge questions with third parties.
- d. Participant will provide up-to-date contact information, including email addresses and cell phone numbers to Greenleaf.
- e. Participant has enrolled in two-factor authentication and account alerts, as available, on their accounts.
- f. Participant has installed current software updates on their devices.
- g. In the event Participant suffers identity theft, Participant will change their account passwords and notify Greenleaf immediately.
- h. Plan Sponsor will cooperate in any investigation of fraud or Cybersecurity Event, including but not limited to completing an affidavit of fraud, filing a police report, and/or providing Greenleaf's investigative team access to computer or email logs.

iv. Fraud Restoration Limitations. Fraud restoration does not cover direct or indirect losses arising from the following:

- a. Activity by Plan Sponsor, financial advisor, or other untrusted third party who is authorized by Participant to access data or with whom a Participant has shared their account credentials.
- b. A breach, security compromise, or cybersecurity event of the systems of those third parties (as referenced in point "a" above).
- c. Accounts held or managed by third parties, such as outside self-directed brokerage accounts.
- d. Taxes, legal fees, expenses or any indirect, consequential, or non-monetary damages or those amounts that have already been reimbursed from other sources, such as identity theft insurance.
- e. Unauthorized use of a Password occurring before Greenleaf is notified that a Password is compromised, unless such unauthorized use is the result of Greenleaf's negligence or willful misconduct.
- f. Losses that result from Participant's own negligence, or from Plan Sponsor's negligence or breach of fiduciary duty.

[END]