Customer Protection for Retirement Plan Accounts at The Standard

Information security is a top priority at The Standard. We value your trust and have safeguards in place to keep your confidential information and retirement account secure. You can take further steps to protect your account, and if you do, The Standard makes this promise:

If assets are removed from your retirement plan account due to unauthorized activity after you have taken the actions below to protect your information and your account, The Standard will reimburse your retirement plan account in the amount of the unauthorized withdrawal.

How do I get Customer Protection for my retirement account?

If you have a retirement plan account with The Standard and take the actions below, you are eligible for Customer Protection.

What is covered under this protection?

This protection covers the cash distributed from your retirement plan account with The Standard. This includes 401(k), profit sharing, 403(b) and 457 plans for which The Standard is the recordkeeper.

What actions must I take to be eligible for Customer Protection?

To be eligible for this protection, you must:

- Create a Personal Saving Center account. Here are instructions to set up your online account in English and Spanish
- Set up Multifactor Authentication on your Personal Savings Center account (a second layer of security, which requires a one-time PIN with login)
- Regularly review all communications from The Standard for accuracy, including quarterly statements, and contact us immediately upon finding any inaccurate or suspicious information.
- Have up-to-date contact information on your account
- Notify The Standard *as soon as possible* if you notice or suspect your account is compromised, or if you see any unauthorized transaction or activity in your account
- Not be at fault for the distribution. Being at fault for a fraudulent distribution includes, but is not limited to:
    - Sharing your Personal Savings Center username, password or security questions with others
    - Failing to promptly respond to account notifications from us

What do I do if I see or suspect unauthorized activity on my account?

If you suspect unauthorized activity, errors or discrepancies on your account, contact us immediately at 800.858.5420. You should also contact us if you have not received your account statement as expected, or if the device you normally use to access your account or contact us is lost or stolen.

How do I submit a claim for this protection?

You must provide notice to The Standard as soon as possible after you notice or suspect a compromise to your account to be eligible for this protection. If you notice *any* compromise to your account, contact us immediately at 800.858.5420. We will provide you with a claim form and ask for your cooperation with any investigation (including filing a police report). Once we have received your claim form and a copy of the police report, we will evaluate your eligibility for the protection.[1] If you are eligible, your account will be reimbursed for the loss.

What is not covered by this protection?

If you voluntarily share your account information with any persons or entities, their activity is considered authorized by you and is not covered by this protection. Also not covered is activity resulting from misuse, negligence, use of malware, security breach, or fraud by an employer/plan administrator, financial intermediary or third party authorized by you to access or to receive your data or with whom you've shared your username, password or account number. The protection does not cover taxes, legal fees, lost opportunity costs, interest or consequential/non-monetary damages, unless otherwise prohibited by applicable laws. The customer protection will not cover amounts that have been or are eligible to be reimbursed, for example, through insurance.

What other ways can I protect my account?

Keep Your User Name and Password Secure

- Never share your password with anyone. We will never ask you for this information over the phone or via email.
- Use a unique password for each of your online accounts.
- Consider using a phrase for your password, or increase its length, to make it harder to guess.
- Do not use any personal information such as your Social Security number, date of birth or wedding date as part of your password or user name.

Review Your Account Information Regularly

- Make sure the contact information in your online profile is up to date. This will help us verify your identity and contact you when necessary.
- Regularly review your account activity. If you see something that doesn't look right, contact us immediately at 800.858.5420.

Be Aware of Scamming Techniques

- Watch out for "phishing" emails that attempt to trick you into clicking on a link or opening an attachment. Never open attachments that you weren't expecting or click on links to websites you don't recognize.
- Beware of imposter websites that may look similar to legitimate websites. Never submit information from a web address that starts with "http" instead of "https." When in doubt, you can always access your account from links on our secure website: https://www.standard.com.

[1] The Standard will investigate and in its sole discretion determine whether eligibility criteria are met and the amount of reimbursement.

- Be cautious of the network you use to connect when you’re not at home. Some criminals will set up their own networks in an attempt to lure you into using them. This can allow them to access your private information. If you aren’t sure whether a network is legitimate, ask a representative at the location where you’re connecting.

Protect Your Devices

- Update the software on your devices regularly to make sure they receive the latest security patches. Use the auto update feature, if available, to make this easier.
- Prevent unauthorized access to your devices by using a personal firewall, latest anti-virus and anti-malware software and using your device’s lock screen security feature. Many manufacturers can recommend what works best with their devices.
- If you’re not using a device, turn it off. This will shut off any Internet connections that an intruder could use to access it. If you’re stepping away from it temporarily, use the lock screen.
- Install software only from reputable sites. If software starts to install itself and you do not recognize the name of the software, deny the installation.
- Remove all personal information from your devices before selling, donating or discarding them.

RP **21629** (6/24)