Your Security Online

AIG takes privacy and data security very seriously

AIG continuously assesses the aig.com/annuities security environment to find and mitigate weaknesses and monitor and respond to threats we detect. You personally can also take steps, such as those outlined below, to protect yourself when online with any company, when using email, and on phones.

Shared computers

When using a shared or public computer:

- Don't check "remember my ID on this computer" option for any website.
- Sign out of any logged on session when finished.
- Watch for onlookers who can see you type passwords.
- Clear browsing history data (see your web browser's help guide on how to clear cache).

Preventing fraud

- Never provide personal information on unfamiliar websites or to people you do not know in person, via email or over the phone, unless you initiated the contact and are sure about with whom you are dealing. Fraudsters often pose as representatives of banks, credit card companies or other service providers.
- Be aware that email scams often create a sense of urgency to respond or advise that you will lose access if you do not provide information.
- If you believe you have given out information to a suspicious party, don't hesitate to contact your financial institutions, including AIG, so they can help you protect your accounts.
- Review statements and credit reports frequently to identify suspicious activity.

Identity theft

- Keep your information private and never post it on social media.
- Don't respond to chain emails, unsolicited emails or emails from unknown people. Don't link to websites within emails as they may be decoy sites trying to capture personal information.
- If you believe your identity has been compromised, contact us, the Federal Trade Commission and your other financial institutions.
- If you believe your email account has been hacked, notify us and your other financial institutions.

Computer protection

- Keep antivirus and other installed software current with updates.
- Be careful when opening email attachments. Scan them with antivirus software before opening.
- Don't install unfamiliar apps. Only obtain software from trusted sources.
- Don't click on pop-ups to close them — use Ctrl+W (for Windows OS).
- Call a professional if you think your computer is infected.

Account security

Public networks

- Assume any information sent can be read. Use encrypted websites for communication on public networks.
- Look for "https://" versus "http://" in the URL. The "s" indicates that the connection is secure.
- Refrain from entering personal information or discussing personal matters on public internet access (e.g., coffee shops, airports, hotels); others may be able to view your information.
- If you must use a public network, use a Virtual Private Network (VPN) to help ensure privacy.

Phishing

- Be wary of email or instant messages asking you to sign in or enter private information.
- If unsure about the legitimacy of a website, manually type the URL into your browser's address bar (instead of clicking a link).
- If unsure of the authenticity of a website, provide a fake password. If it appears you are authenticated, you are likely on a phishing website.
- Look for misspelled words or other clues that may indicate a fake.

Online & mobile security

- Download apps from trusted locations (e.g., Apple or Google app stores).
- Treat smartphones and tablets with the same security as a personal computer.
- Use antivirus and firewall software security tools and keep devices up to date.
- Use the screen lock on your mobile device.
- Change passwords often and use strong ones [combination of both uppercase (A-Z) and lowercase (a-z) letters, numbers (0-9), and special characters. (@ . _)]. Do not use the same password across multiple sites or devices.
- Never share login credentials or passwords.

Reporting security issues

If you have a security concern regarding one of your accounts, please contact us.
A representative will assist in addressing your concerns and working toward resolution.

M5811FL1 (11/17)