Life

NORTH AMERICAN®
A Sammons Financial Company
North American Company for Life and Health Insurance®

Field Bulletin

Cybersecurity and privacy best practices

493NB

Like you, we continue to hear about data breaches in the news and we want to help you protect your (and your customers') data and personal information. While our Company has not been the subject of a data breach, we know that producers have been targeted given the large amount of personally identifiable information they safeguard. Once a fraudster has your customers' information, they will then try to attack all of their accounts. We've also been notified recently by some of our producers that their email addresses were compromised following data breaches with other online entities, so it's important that you be vigilant and that we share some best practices:

Email Addresses and Passwords

- Avoid weak or easily guessed passwords. Your password should be a combination of letters, numbers, and symbols that is not easily guessed. The current guidance is for your email password to be 14-16 characters long.
- Your password could have been obtained by a fraudster through a public breach. Some of the best practices to consider when using other companies to manage your accounts is to make sure you change your passwords frequently. Cybersecurity experts recommend changing your passwords every 3 months.
- Your information could also have been exposed if you have inadvertently clicked on a malicious link in an email, social networking site, or webpage.

Best Practices

- If you have the ability to use Multi-Factor Authentication ("MFA") to protect your email or your other accounts, use it. MFA is one of the better ways to protect your email account information and everything your email contains. MFA is typically utilized by sending a text message to a known cell phone number and issuing a code, followed by you entering that code to verify authenticity.
- Do not send confidential information over unencrypted email, including, but not limited to, customers' dates of birth, Social Security Numbers, phone numbers, addresses, and account/policy/contract numbers.
- Educate your office about best practices as well.
- Ensure that you have current, up to date antivirus software installed to prevent malware. Be sure to regularly install patches and updates to your devices.
- Consider having your computer evaluated by a computer expert to confirm there is no malware or spyware lurking in the background.

If you believe you have been affected by a data breach, please notify our Company immediately so that we can determine next steps (and we would strongly recommend you consult with a computer expert to clear your system of any possible malware and/or spyware). If your customer alerts you that their information has been breached, notify us immediately so that we can take prompt action to add additional safeguards against fraudulent withdrawal attempts.

Thank you in advance for you due diligence in keeping your (and our shared customers') information safe.