Bug Reporting Terms

OneAmerica Financial

Introduction

This document is intended to provide terms for security researchers to report bugs, including what systems and types of research are covered, how to send us vulnerability reports, and how long security researchers should wait before publicly disclosing vulnerabilities.

Authorization

If you make a good faith effort to comply with all guidelines listed herein during your security *research*, we will consider your research to be authorized. We will work with you to understand and resolve the issue quickly, and OneAmerica Financial will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with the terms herein, we will make this authorization known.

Guidelines

"Research" means activities in which you:

- **Act in good faith.** Notify us as soon as possible after you discover a real or potential security issue.
- **Respect privacy.** Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- **Tread lightly.** Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- **Work with us.** Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- **High impact reports only.** Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately via https://oneamerica.tfaforms.net/96, and not disclose this data to anyone else**.

Test methods not authorized

The following test methods are **NOT** authorized, and will be subject to legal action:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data; or
- Physical security testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.

Scope

The scope applies exclusively to the following systems and services:

- *.oneamerica.com
- *.aul.com

Any service not expressly listed above, such as any connected services, are excluded from scope and are NOT authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of the scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at **applicationsecurityteam@oneamerica.com** before starting your research.

Although we develop and maintain other internet-accessible systems or services, we ask that *active research and testing* not be conducted on any systems and services not covered by the scope of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first. We reserve the right to modify the scope at any time.

Reporting a vulnerability

Information submitted under the terms herein will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely OneAmerica Financial, we may share your report at our discretion with the impacted entity(ies) with whom OneAmerica Financial has a relationship(s), where it will be handled under their security policy. We will not share your name or contact information without express permission.

We accept vulnerability reports at https://oneamerica.tfaforms.net/96. Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 3 business days.

By submitting a vulnerability, you acknowledge that you have no expectation of payment and that you expressly waive any future pay claims against OneAmerica Financial related to your submission

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the location where the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Recommended solution (optional, but appreciated)
- Be written in English, if possible.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within 3 business days, we will acknowledge that your report has been received, if submitted with your contact information.
- To the best of our ability, and in accordance with applicable laws and regulations, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

Questions

Questions regarding this policy may be sent to **applicationsecurityteam@oneamerica.com**.

Document change history

Version	Date	Description
1.0	January 22, 2025	Initial Publication
1.1	October 1, 2025	Minor Revision