directly

Directly Bug Bounty Program

Rewards

We maintain flexibility with our reward system. Our minimum reward is $250 US and there is no maximum; rewards are based on severity and impact.

To be eligible for a reward, the exploit must rely on vulnerabilities of Directly's systems. Rewards are only available for bugs that can be used by itself or in combination with another vulnerability you report to access data that is not yours.

If we receive multiple reports for the same vulnerability, only the person offering the first clear report will receive a reward.

Rewards are paid through Paypal. The beneficiary is responsible for all taxes, fees, and tariffs in their country of residence.

To receive a reward, you must reside in a country not on sanctions lists (e.g., Cuba, Iran, North Korea, Sudan & Syria).

Reproducibility

Our engineers must be able to reproduce the security flaw from your report. Reports that include clearly written explanations and working code are more likely to garner rewards.

Responsible Disclosure

Security of user data and communication is of the utmost importance to Directly. In pursuit of the best possible security, we welcome responsible disclosure of any vulnerability you find. Principles of responsible disclosure include:

- Do not extract data from our infrastructure (including customer data, source code, data backups, configuration files).
- If you obtain access to our system, report your finding immediately. Do not attempt to pivot to other servers or elevate access.
- Avoid scanning techniques that are likely to cause degradation of service to customers (e.g. by overloading the site). This includes the spamming of contact forms, support emails, etc.
- Keep details of vulnerabilities secret for at least 60 days such that Directly has had a reasonable amount of time to remediate the vulnerability.

Examples of Qualifying Vulnerabilities

- Authentication flaws
- Circumvention of our Platform/Privacy permissions model
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF/XSRF). This excludes logout CSRF.
- Server-side code execution