Responsible Vulnerability Disclosure Policy

Policy Owner: CTO

Effective Date: 2025-11-14

At CloudCard, we welcome feedback regarding security weaknesses in our products. Security researchers or other concerned citizens may report potential security vulnerabilities via email to support@cloudcard.us with the subject "**Responsible Vulnerability Disclosure**".

Disclosure Policy

- Please provide us with a reasonable amount of time to remediate the vulnerability before making the finding public or disclosing to a third party.
- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading CloudCard services. Only interact with accounts you own or for which you have explicit permission from the account holder.
- If you make a good faith effort to comply with this policy 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 CloudCard 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 this policy, we will make this authorization known.

Exclusions

While researching, do not engage in:

- Denial-of-Service (DoS)
- Spamming
- Social engineering or phishing of CloudCard employees or contractors
- Any attacks against CloudCard's physical property or data centers

This policy applies to CloudCard operated applications hosted at RemotePhoto (US) and RemotePhoto (CA), any other subdomains or services associated with these environments, as well as our test environment. Note, CloudCard provides or operates additional customer and partner specific environments of our software - please obtain permission from the relevant customer or partner before performing research against those environments.

We do not accept reports for vulnerabilities solely affecting our marketing website (https://www.remotephoto.ai/) which contains no sensitive data. In addition, reports that describe theoretical attack vectors without substantiated proof of exploitability are excluded.

Rewards

At our present scale and program maturity, we do not offer financial rewards.

We are willing to provide public recognition, with your consent, by adding your name to our CloudCard Responsible Disclosure Acknowledgements Confluence page.

Additionally, we love disc golf, so we are also willing to commemorate your efforts with a custom CloudCard Bug Bounty disc as a trophy for your work. If we determine your disclosure is worthy of a disc, we will contact you for a mailing address at which you can receive a package.

Process

When we receive a disclosure:

1. the CloudCard Security Team will acknowledge receipt of the disclosure (so you know you have been heard). This may take up to 5 business days, although we aim to respond significantly faster.
2. Security Engineers will evaluate the accuracy, novelty, impact and severity of the disclosure.
3. If we determine that the disclosure is meaningful, we will assign a vulnerability identifier and a severity level to the disclosure.

In response to a disclosure, we will provide you the following information:

1. acknowledgement that we have received the disclosure
2. guidance regarding how much time we need before the disclosure is be made public
3. as much information as we deem safe to provide, given the circumstances of the specific disclosure.

Once the disclosure has been resolved, we will contact you regarding rewards, as described above.

Version	Date	Description	Author	Approved by
1.0	2025-11-14	First Version	Ryan Heathcote	Jonathan Hoffman