IPSY Vulnerability Disclosure Policy

Personalized Beauty Discovery, Inc. ("IPSY") takes the security of our systems seriously, and we value the security community. The disclosure of security vulnerabilities helps us ensure the security and privacy of our users. Because of this, IPSY encourages the security community to communicate such vulnerabilities to us, provided that you follow the protocols below.

We require that all researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing;
- Perform research only within the scope set out below;
- Use the identified communication channels to report vulnerability information to us; and
- Keep information about any vulnerabilities you've discovered confidential between yourself and IPSY until we've had 90 days to resolve the issue.

If you follow these guidelines when reporting an issue to us, we commit to:

- Not pursue or support any legal action related to your research;
- Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 72 hours of submission);
- Reward you with a $200 bounty, paid via bank wire transfer, if you are the first to report a particularly significant security vulnerability; we do not offer financial compensation for reports of minor issues or for vulnerabilities we are already aware of through internal testing/scanning or other means.

In the interest of the safety of our users, staff, the Internet at large, and you as a security researcher, the following test types are excluded from scope:

- Findings from physical testing such as office access (e.g. open doors, tailgating)
- Findings derived primarily from social engineering (e.g. phishing, vishing)
- UI and UX bugs and spelling mistakes
- Network level Denial of Service (DoS/DDoS) vulnerabilities

Things we do not want to receive:

- Personally identifiable information (PII)
- Credit card holder data

If you believe you have found a security vulnerability in one of our sites or apps, please send it to us by emailing security@ipsy.com. Please include the following details with your report:

- Description of the location and potential impact of the vulnerability;
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us);
- Your full name and contact information, including your mobile number); and
- IRS Form W-9 or W-8, depending on your country of residency, for any bounty payment.