Vulnerability disclosure policy

We welcome reports from people who find a security weakness in an Olympus service.

Version 1.0. Published 20 September 2026.

How to report

Email security@olympuspay.co. Include what you found, where you found it, the steps to reproduce it and the impact you believe it has. Please keep the report confidential until we have had the chance to fix it.

In scope

- The Olympus websites, including olympuspay.co and the developer site
- Online banking and the merchant dashboard
- The Olympus mobile apps and the public Olympus API

The rules

- Use only your own accounts and data. Do not access, change or delete another customer's data
- Do not disrupt the service: no denial of service, load testing or spam
- Do not use social engineering, phishing or physical attacks against Olympus staff or customers
- Stop and report as soon as you reach personal data. Do not copy or keep it
- Do not make a vulnerability public before we have fixed it

What we will do

We will acknowledge your report, look into it and keep you informed of progress. We will not pursue legal action against researchers who follow this policy in good faith. This policy does not promise a reward.

Not covered

Reports about services run by other companies, weaknesses that need physical access to a device, and issues found by testing outside this policy.