Responsible Disclosure

Last updated: 2026-06-25 Classification: Public.

DealTracker welcomes reports of suspected security vulnerabilities in its production systems. We investigate every good-faith report and work with the reporter through to remediation.

How to report

Send reports to security@getdealtracker.com. Researchers whose tooling expects a machine-readable contact can find one at https://getdealtracker.com/.well-known/security.txt. To let us reproduce and assess the issue quickly, please include a description of the vulnerability and its impact, step-by-step reproduction instructions identifying the affected URL or endpoint, and any supporting material such as a proof of concept, request and response pairs, or screenshots.

Our commitment to good-faith research

- We acknowledge every report within two business days.
- We triage each report through our incident-response process, prioritize by severity, and provide status updates through to remediation.
- Safe harbor: we will not pursue or support legal action against researchers who act in good faith, remain within the scope below, avoid privacy violations and service degradation, and allow us a reasonable opportunity to remediate before disclosing. If a third party brings action against a researcher for in-scope, good-faith work conducted under this policy, we will confirm that the activity was authorized.

DealTracker does not operate a paid bug-bounty program at this time. Public acknowledgment is available on request once an issue has been resolved.

Scope

In scope: the DealTracker production application at getdealtracker.com and its production API. We give priority to vulnerabilities affecting customer matter data, authentication and session handling, tenant isolation, access control, and the AI write path.

Out of scope

The following are out of scope: denial-of-service and volumetric testing; social engineering; physical attacks; vulnerabilities in third-party providers (Microsoft Azure, Auth0/Okta), which should be reported to those providers directly; accessing, altering, or exfiltrating data that does not belong to you; automated scanning that generates excessive traffic; and findings with no demonstrated security impact, such as missing best-practice headers absent a concrete exploit. Please do not disclose a report publicly until we have remediated the issue and agreed on timing with you.

Contact

- Security: security@getdealtracker.com (machine-readable contact at https://getdealtracker.com/.well-known/security.txt)
- Privacy and data protection: privacy@getdealtracker.com

This page is not a contract. Where it differs from the signed agreement or DPA, those govern.