Global Payments Vulnerability Research Program ("VRP") Policy

Global Payments Inc. ("Global Payments") looks forward to working with the information security community to find vulnerabilities in order to keep our businesses and customers safe. Please read this Program Policy in its entirety.

Global Payments Information Security

The information security team at Global Payments is devoted to being a trusted security and assurance partner across the enterprise.

Part of our vision is to develop and enable the organization to proactively identify and mitigate information security risk to our assets and to evolve our core information security foundation. The VRP will be a key element in achieving these goals.

Eligibility for Participation

- You must be 18 years old or older to submit a vulnerability for consideration. If you are a minor, you must submit through a parent or legal guardian.
- You must be an individual security researcher participating in your own individual capacity.
- If you work for a security research organization, that organization must permit you to participate in your individual capacity. You are responsible for reviewing your employer's rules for participating in the VRP.

Ineligibility for Participation

You may not participate in the VRP if you are any of the following:

- A resident of any country/region that is under United States sanctions, such as Cuba, Iran, North Korea, Sudan, and Syria or Crimea, or a person designated in the U.S. Department of the Treasury's Specially Designated Nationals List.
- A current employee of Global Payments Inc., a Global Payments affiliate, or an immediate family member (parent, sibling, spouse, or child) or household member of such an employee.
- A contingent staff member, contractor, or vendor employee that is currently working with, or has worked in the past twelve (12) months with, Global Payments Inc. or a Global Payments affiliate.

Response Targets

Global Payments will make a best effort to meet the following SLAs for security researchers participating in the VRP:

Type of Response	SLA in business days
First Response	2 days
Time to Triage	2 days
Time to Resolution	depends on severity and complexity

We'll try to keep you informed about our progress throughout the process.

Assets in Scope

All assets associated with our core enterprise are considered in scope. No VPN access nor credentials will be provided for testing.

Disclosure Policy

You agree not to discuss any vulnerabilities (even resolved ones) outside of the VRP without express consent from Global Payments.

Global Payments reserves the right to approve or deny any request for disclosure.

You agree to follow HackerOne's disclosure guidelines.

Program Rules

- Please provide detailed reports with reproducible steps. If the report is not sufficiently detailed to enable reproduction of the issue, the issue may not be triaged.
- Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact.
- When duplicates occur, we only triage the first report that was received (provided that it can be fully reproduced).
- Multiple vulnerabilities caused by one underlying issue will be treated as one valid report.
- Social engineering (e.g. phishing, vishing, smishing) is prohibited.
- Only interact with accounts you own or with explicit permission of the account holder.
- Do not engage in any activity that can potentially or actually cause harm to Global Payments, our customers, or our employees.
- Do not engage in any activity that can potentially or actually stop or degrade Global Payments' services or assets.
- Do no harm and do not exploit any vulnerability beyond the minimal amount of testing required to prove that a vulnerability exists or to identify an indicator related to a vulnerability.
- Do not store, share, compromise or destroy Global Payments or our customer data. If Personally Identifiable Information (PII) is encountered, you should immediately halt your activity, purge related data from your system, and contact Global Payments. This step protects any potentially vulnerable data, and you.
- Do not initiate a fraudulent financial transaction.

Out of Scope Vulnerabilities

When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug. The following issues are considered out of scope:

- Unexploitable vulnerabilities discovered via scanning. All submissions must have a valid proof of concept
- Any activity that could lead to the disruption of our service (DoS/DDOS).
- Clickjacking on pages with no sensitive actions
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions
- Attacks requiring MITM or physical access to a user's device.
- Previously known vulnerable libraries without a working Proof of Concept.
- Comma Separated Values (CSV) injection without demonstrating a vulnerability.
- Missing best practices in SSL/TLS configuration.
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS
- Rate limiting or bruteforce issues on non-authentication endpoints
- Missing best practices in Content Security Policy
- Missing HttpOnly or Secure flags on cookies
- Missing email best practices (Invalid, incomplete or missing SPF/DKIM/DMARC records, etc.)
- Vulnerabilities only affecting users of outdated or unpatched browsers (Less than 2 stable versions behind the latest released stable version)
- Software version disclosure / Banner identification issues / Descriptive error messages or headers (e.g. stack traces, application or server errors).
- Tabnabbing
- Open redirect - unless an additional security impact can be demonstrated
- Issues that require unlikely user interaction

Grounds for Disqualification

Attempting any of the following could result in permanent disqualification from the VRP and possible criminal and/or legal investigation. We do not allow any actions that could negatively impact the experience on our websites, apps, or other assets for other Global Payments customers.

- Disruption or denial-of-service attacks (Application and Network)
- Social engineering attacks
- Brute-force attacks
- Exfiltration of data
- Code injection on live systems
- The compromise or testing of application accounts that are not your own
- Any threats, attempts at coercion, or extortion of Global Payments employees, other partner employees, or customers
- Physical attacks against Global Payments, contractors, or customers
- Any physical attempts against Global Payments property or data centers
- Access the personal information of any other person without consent
- Any other action that violates the law
- Any action that endangers yourself or others
- Aggressive vulnerability scans or automated scans on Global Payments servers (including scans using tools such as Core Impact or Nessus)
    - Keep scans to 45 requests per minute

globalpayments

Legal

You must otherwise comply with all applicable Federal, State, and local laws, regulations, and rules in connection with your security research activities. You may not engage in any security research or vulnerability disclosure activity that is inconsistent with terms and conditions of the VRP or the law. If you engage in any activities that are inconsistent with the terms and conditions of the VRP or the law, you will not be considered a security researcher and may be subject to criminal penalties and civil liability. Global Payments reserves all rights against any illegal use of the reported vulnerability information.

Any Global Payments information that you may encounter, view, acquire, or access, is owned by Global Payments or its customers, clients, or third-party providers. You have no rights, title, or ownership in any such information. Nothing in this Program Policy shall be deemed to constitute the grant to you of any license or other right to or in respect of any Global Payments or third-party product, service, patent, trademark, trade secret, or other intellectual property.

You have no obligation to provide Global Payments with the abovementioned security and vulnerability information. By submitting such information to Global Payments, you are indicating that you have read, understand, and agree to the terms and conditions of this Program Policy. Further, you agree that by submitting such information to Global Payments, even if the information is not eligible for a reward, you grant Global Payments a worldwide, perpetual, irrevocable, non-exclusive, transferable, sublicensable, fully-paid and royalty-free license under any and all intellectual property rights that you own or control to use, copy, modify, create derivative works based upon and otherwise exploit such information for any purpose.

Global Payments may modify the terms and conditions or terminate the VRP at any time.

Safe Harbor

Activities conducted in a manner consistent with this policy will be considered authorized conduct, and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Submission Instructions

Global Payments uses HackerOne to triage and validate responsibly disclosed vulnerability reports. Please submit your report via HackerOne: https://hackerone.com/global-payments.

Thank you for helping to keep Global Payments and our users safe!