globalpayments

Vulnerability Disclosure Program "VDP" Policy

January, 2026

Contents

globalpayments

Introduction.

Global Payments is a leading payments technology company delivering innovative software and services to merchant and issuer customers globally. Global Payments looks forward to working with the information security community to find vulnerabilities in order to keep our businesses and customers safe. To achieve this, a Vulnerability Disclosure Program “VDP” policy has been defined in this document which outlines the rules of engagements for researchers participating in the VDP. Global Payments VDP is hosted through HackerOne and all researchers (“hackers”) must be registered and report findings through this channel.

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 Program.

Ineligibility for Participation

You may not participate in the Program if you are any of the following:
A resident or have a tax form from China or Hong Kong. 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 response targets for researchers participating in our program:

Type of Response	Response Target
First Response	2 days
Time to Triage	2 days
Time to Bounty	14 days
Time to Resolution	depends on severity and complexity

We will try to keep you informed about our progress throughout the process. Please note, however, that numerous circumstances, including but not limited to resource constraints, a high volume of submissions, intervening public holidays, and more may interfere with our ability to meet these response targets, and that you are obligated to continue to comply with all of the Program Guidelines even if we do not respond on time.

Test Plan

Keep scans to 45 requests per minute

1) For account creation, use your HackerOne email address and only create a single user account.

2) See assets in scope for specific instructions on testing.

Disclosure Policy

By participating in the program, you agree not to discuss or disclose any vulnerabilities (even resolved ones) outside of the Program without express prior consent from Global Payments.

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

- You agree to follow HackerOne's disclosure guidelines.

Program Guidelines

- This program is not intended to encourage any researcher to access or view any of the following sensitive forms of data, each of which is subject to stringent legal protections: (1) Personal Information, defined here to include any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household; or (2) any Payment Account Number (PAN), Cardholder Data (CHD), or Sensitive Authentication Data (SAD), as each term is defined by the Payment Card Industry Data Security Standard (PCI-DSS). Should you encounter any such information during your research, you must immediately halt your activity and contact Global Payments, and you must purge any such data from your system(s) following the submission of your report. Adhering to these requirements protects both Global Payments and you.

- 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 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.
In addition to the below any vulnerability on the HackerOne Core Ineligible Findings list is out of scope:

- Unexploitable vulnerabilities discovered via scanning. All submissions must have a valid proof of concept
- Attacks requiring MITM or physical access to a user's device
- Vulnerabilities on partner or supplier products
- Rate limiting or bruteforce issues on non-authentication endpoints

Grounds for Disqualification

Because we do not allow any actions that could negatively impact the customer experience on our websites, apps, or other Global Payments assets, attempting any of the following could result in permanent disqualification from the Program and could result in a possible criminal and/or legal investigation:

- 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
- Any other action that violates these Program Guidelines
- 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)

Legal Terms

By submitting security or vulnerability information to Global Payments, you confirm that you have read, understand, and agree to these Program Guidelines. 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, or create derivative works based upon such information and otherwise exploit such information for any purpose.

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 these Program Guidelines shall be deemed to constitute a grant of any license or other right to or in any Global Payments or third-party product, service, patent, trademark, trade secret, or other intellectual property.

You must comply with all applicable federal, state, local, and international laws, regulations, and rules in connection with your security research activities. If you violate any applicable law or any requirement established by these Program Guidelines, you will not be considered a security researcher, and you may become subject to criminal penalties and civil liability. In particular, by participating in the Program, you confirm your understanding: (1) that applicable federal laws make it a felony offense for you to intentionally access an information system that is connected to the internet without authorization, or to exceed the scope of your authorized access to such a system, and in doing so to obtain any information therefrom; and (2) that any action that you take on a Global Payments information system that exceeds the limits established by these Program Guidelines may therefore constitute a federal crime. Global Payments reserves all rights to pursue all available remedies, civil and criminal, against any individual or entity operating in excess of the Program Guidelines.

Global Payments retains the right to obtain your Personal Data (as defined in the HackerOne Privacy Policy) from HackerOne, and to process such Personal Data, as necessary to accomplish the legitimate business objectives of Global Payments, including but not limited to ensuring the security and integrity of our infrastructure, data, products, and services. Global Payments may also obtain and process your Personal Data for the purpose of exercising or defending legal rights; to take precautions against liability; to protect the rights, property, or safety of Global Payments, of any other individuals, or of the general public; to protect Global Payments and our assets from fraudulent, abusive, or unlawful uses; or to investigate and defend Global Payments against third-party claims or allegations. By submitting a vulnerability report via the Global Payments VDP (https://hackerone.com/global-payments) you consent to HackerOne sharing Personal Data with Global Payments, upon request, in the circumstances described in this paragraph.

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

Safe Harbor

Any research activities conducted in strict accordance with these Program Guidelines, as determined by Global Payments, will be considered authorized conduct, and we will not initiate legal action against you relating to such research activities.

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