Security at Stripe

Our users trust Stripe with their sensitive data and rely on us to be good custodians of their customers' data as well. As a payments infrastructure company, our security posture continually evolves to meet the rigorous standards of the global financial industry.

Standards and regulations compliance

Stripe uses best-in-class security practices to maintain a high level of security.

PCI-certified

A PCI-certified auditor evaluated Stripe and certified us to PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry. This audit includes both Stripe's Card Data Vault (CDV) and the secure software development of our integration code.

We provide our users with features to automate some aspects of PCI compliance.

- We analyze the user's integration method and dynamically inform them of which PCI validation form to use.
- If a user integrates with Stripe Elements, Checkout, Terminal SDKs, or our mobile libraries, we provide assistance in completing their PCI validation form (Self-Assessment Questionnaire A) in the Dashboard.
- We publish a PCI Compliance Guide to help educate our users about PCI compliance and how Stripe can help.

System and Organization Controls (SOC) reports

Stripe's systems, processes, and controls are regularly audited as part of our SOC 1 and SOC 2 compliance programs. SOC 1 and SOC 2 Type II reports are produced annually and can be provided upon request.
The Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) Trust Service Criteria (TSC) developed the SOC 3 report. Stripe's SOC 3 is a public report of internal controls over security, availability, and confidentiality. View our recent SOC 3 report.

EMVCo standard for card terminals

Stripe Terminal is certified to the EMVCo Level 1 and 2 standards of EMV® Specifications for card and terminal security and interoperability. Terminal is also certified to the PCI Payment Application Data Security Standard (PA-DSS)—the global security standard that aims to prevent payment applications developed for third parties from storing prohibited secure data.

NIST Cybersecurity Framework

Stripe's suite of information security policies and their overarching design are aligned with the NIST Cybersecurity Framework. Our security practices meet the standards of our enterprise customers who must provide secure products like on-demand cloud computing and storage platforms (for example, DigitalOcean and Slack).

Privacy and data protection

We continuously implement evolving privacy and data protection processes, procedures, and best practices under all applicable privacy and data protection regimes. For more information, see the following resources:

- Privacy policy
- Privacy center
- Data processing Agreement

Stripe product securement

Security is one of Stripe's guiding principles for all our product design and infrastructure decisions. We offer a range of features to help our users better protect their Stripe data.

Sensitive action authentication

The Stripe Dashboard supports several forms of multi-factor authentication (MFA) including: SMS, time-based one-time password algorithm (TOTP), and universal 2nd factor (U2F). We also support single sign-on through Security Assertion Markup Language (SAML) 2.0, allowing customers to mandate sign-in requirements, configure access control, and instantly onboard team members through Just-in-Time account provisioning.

Support requests from users must be authenticated by sending the request from the Dashboard (after login) or by verifying account access before a support response is proffered. By requiring authentication, we minimize the risk of providing any information to non-authorized people.

Access restriction and auditing

From the Dashboard, users can assign different detailed roles to enable least-privilege access for their employees, and create restricted access keys to reduce the security and reliability risk of API key exposure.

Users can also view audit logs of important account changes and activity in their security history. These audit logs contain records of sensitive account activity, like logging in or changing bank account information. We monitor logins and note:

- If they're from the same or usual devices
- If they're from consistent IP addresses
- Failed attempts

Users can export historical information from the logs. For time-sensitive activities, such as logins from unknown IPs and devices, we send automatic notifications so that logs don't need to be reviewed manually.

HTTPS and HSTS for secure connections

We mandate the use of HTTPS for all services using TLS (SSL), including our public website and the Dashboard. We regularly audit the details of our implementation, including the certificates we serve, the certificate authorities we use, and the ciphers we support. We use HSTS to make sure that browsers interact with Stripe only over HTTPS. Stripe is also on the HSTS preloaded lists for all modern major browsers.

All server-to-sever communication is encrypted using mutual transport layer security (mTLS) and Stripe has dedicated PGP keys for users to encrypt communications with Stripe, or verify signed messages they receive from Stripe. Our systems automatically block requests made using older, less secure versions of TLS, requiring use of at least TLS 1.2.

The stripe.com domain, including the Dashboard and API subdomains, are on the top domains list for Chrome, providing extra protection against homoglyph attacks. This makes it harder to create fake pages that look like stripe.com in Chrome (for example, strípe.com), which renders as punycode (xn–strpe-1sa.com), in turn making it harder for Stripe credentials to be phished.

Proactive internet monitoring

We proactively scan the internet for our merchants' API keys. If we find a compromised key, we take appropriate action, advising the user to roll their API key. We use the GitHub Token Scanner to alert us when a user's API keys have been leaked on GitHub. If we find external phishing pages that might catch our users, we work proactively with our vendors to take those down and report them to Google Safe Browsing.

Infrastructure safeguards

Our security teams test our infrastructure regularly by scanning for vulnerabilities and conducting penetration tests and red team exercises. We hire industry-leading security companies to perform third-party scans of our systems, and we immediately address their findings. Our servers are frequently and automatically replaced to maintain server health and discard stale connections or resources. Server operating systems are upgraded well in advance of their security end of life (EOL) date.

Dedicated card technology

Stripe encrypts sensitive data both in transit and at rest. Stripe's infrastructure for storing, decrypting, and transmitting primary account numbers (PANs), such as credit card numbers, runs in a separate hosting infrastructure, and doesn't share any credentials with the rest of our services. A dedicated team manages our CDV in an isolated Amazon Web Services (AWS) environment that's separate from the rest of Stripe's infrastructure. Access to this separate environment is restricted to a small number of specially trained engineers and access is reviewed quarterly.

All card numbers are encrypted at rest with AES-256. Decryption keys are stored on separate machines. We tokenize PANs internally, isolating raw numbers from the rest of our infrastructure. None of Stripe's internal servers and daemons can obtain plain text card numbers but can request that cards are sent to a service provider on a static allowlist. Stripe's infrastructure for storing, decrypting, and transmitting card numbers runs in a separate hosting environment, and doesn't share any credentials with Stripe's primary services including our API and website. It's not just PANs that are tokenized this way; we treat other sensitive data, like bank account information, in a similar way.

Corporate technology

Stripe takes a zero-trust approach to employee access management. Employees are authenticated leveraging SSO, two-factor authentication (2FA) using a hardware-based token, and mTLS through a cryptographic certificate on Stripe-issued machines. After connecting to the network, sensitive internal systems and those outside the scope of the employee's standard work require additional access permissions.

We monitor audit logs to detect abnormalities and watch for intrusions and suspicious activity, and also monitor changes to sensitive files in our code base. All of Stripe's code goes through multiparty review and automated testing. Code changes are recorded in an immutable, tamper-evident log. We constantly collect information about Stripe-issued laptops to monitor for malicious processes, connections to fraudulent domains, and intruder activity. We have a comprehensive process for allow listing permitted software on employee laptops, preventing the installation of non-approved applications.

Security posture maintenance

Our developers work with security experts early in a project's life cycle. As part of our Security Review process, security experts develop threat models and trust boundaries that help guide the implementation of the project. Developers use this same process to make changes to sensitive pieces of code.

Dedicated experts on-call

We have a number of dedicated security teams that specialize in different areas of security, including infrastructure, operations, privacy, users, and applications. Security experts are available 24/7 through on-call rotations. We're focused on constantly raising the bar on best practices to minimize cybersecurity risks.

Security is every Stripe employee's job

We require every Stripe employee to complete security education annually, and we provide secure software development training to Stripe engineers. We run internal phishing campaigns to test everyone at Stripe on recognizing phishing attempts and flagging them to the appropriate security team.

Managing access control

We have a formal process for granting access to systems and information; we regularly review and automatically remove inactive access. Actions within the most sensitive areas of the infrastructure need a human review. To enable best practices for access control, our security experts build primitives to assist Stripe teams in implementing the principle of least privilege. To minimize our exposure, we have a data retention policy that minimizes the data we keep while complying with regulatory and business requirements.

Vulnerability disclosure and reward program

We maintain a vulnerability disclosure and reward ("bug bounty") program that compensates independent security researchers who help us keep our users safe. By submitting a security bug or vulnerability to Stripe through HackerOne, you acknowledge that you've read and agreed to the program terms and conditions. Refer to our policy on HackerOne for more information on how to participate in our bug bounty program.