Shopify Inc.

System and Organization Controls

(SOC) 3 Report

Report on Shopify's Ecommerce Platform System for the period
September 1, 2018 to November 30, 2018

Shopify’s Ecommerce Platform

Contents

SECTION I – Shopify’s Management Assertion

150 ELGIN ST., 8th FLOOR
OTTAWA, ONTARIO K2P 1L4

T 1.613.241.2828
F 1.877.350.0829

WWW.SHOPIFY.COM

Shopify's Management Assertion Regarding the Effectiveness of Its Controls Over the Shopify Ecommerce Platform Based on the Trust Services Criteria for Security and Availability

March 15, 2019

We, as management of, Shopify are responsible for designing, implementing and maintaining effective controls over the Shopify Ecommerce Platform system (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the System throughout the period September 1, 2018 to November 30, 2018, to achieve the commitments

and system requirements related to the operation of the System using the criteria for the security and availability (Control Criteria) set forth in the AICPA's TSP section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Based on this evaluation, we assert that the controls were effective throughout the period September 1, 2018 to November 30, 2018 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Shopify's commitments and system requirements
- the System was available for operation and use, to achieve Shopify's commitments and System requirements

based on the Control Criteria.

Our attached description of the boundaries of the Shopify Ecommerce Platform system identifies the aspects of the Shopify Ecommerce Platform system covered by our assertion.

Very truly yours,

Shopify Management

SECTION II – Independent Service Auditor's Report

Ernst & Young LLP
560 Mission Street
Suite 1600
San Francisco, CA
94105-2907

Tel: +1 415 894 8000
Fax: +1 415 894 8099
ey.com

Building a better working world

Independent Service Auditor's Report

To the management of Shopify:

We have examined management's assertion that Shopify maintained effective controls to provide reasonable assurance that:

- the Shopify Ecommerce Platform System was protected against unauthorized access, use, or modification to achieve Shopify's commitments and system requirements
- the Shopify Ecommerce Platform System was available for operation and use to achieve Shopify's commitments and system requirements

during the period September 1, 2018 through November 30, 2018 based on the criteria for security and availability in the American Institute of Certified Public Accountants' TSP section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Shopify's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Shopify's relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Shopify's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security and availability are achieved.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, Shopify's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security and availability.

Ernst & Young LLP

San Francisco, CA
March 15, 2019

SECTION III – Description of Shopify's Ecommerce Platform System

Shopify overview

Shopify is a leading cloud-based, multi-channel commerce platform designed for small and medium-sized businesses. Merchants can use Shopify's software to design, set up, and manage their stores across multiple sales channels, including web, mobile, social media, marketplaces, and physical retail locations. The platform also provides merchants with a powerful back-office and a single view of their business. The Shopify platform was engineered for reliability and scale, making enterprise-level technology available to businesses of all sizes.

Shopify's core Software as a Service (SaaS) offering is a cloud-hosted online storefront, a cloud-hosted checkout process, and a back-end administration portal for merchants to manage customers, products, orders, and other standard business operations, as well as Application Programming Interfaces (APIs) to support these processes.

Scope

Scope inclusions

The scope of this report *includes* systems required to provide the following functionality: For merchants:

- Store: Create an online store that can display web pages to customers and potential customers.
- Admin access: Connect to the store admin using secure transmission.
- Accounts: Manage store staff accounts and permissions.
- Products: Configure product descriptions, prices, discounts, taxes, shipping rates, and inventory.

- **Orders**: View or modify details of completed orders, including fulfilment status, and related financial transactions.
- **Customers**: View, modify or delete customer records.
- **Shopify Payments**: View financial transactions with Shopify Payments.
- **Gift cards**: Configure gift cards (if on an appropriate plan).
- **Support**: Contact 24/7 customer support when help is required.

For customers:

- **Customer access**: Connect to the online store using secure transmission.
- **Shopping cart**: Add one or more products to a shopping cart.
- **Shipping**: Select a shipping method.
- **Checkout**: Complete checkout using Shopify Payments.

Scope exclusions

The scope of this report *excludes* systems required to provide the following functionality:

- **Store management mobile applications**: Shopify store management iOS and Android applications.
- **Point-of-sale**: Shopify POS iOS and Android applications.
- **Fraud analysis**: Shopify's customer fraud detection tool.
- **Analytics**: Analytics visible in Shopify Admin.
- **Shopify data warehouse**: Tool to run Structured Query Language (SQL) queries on customer data.
- **Third-party payment gateways**: Payment gateways other than Shopify Payments.
- **Domains**: Purchase and management of domain records.
- **Shipping**: Buying and printing shipping labels.

- **Opt-in applications**: Platform applications from https://apps.shopify.com.
- **Tax engine**: Third party tax calculations add-on.
- **Credit-card processing**: Shopify's credit card processing environment (covered by PCI-DSS Attestation of Compliance).

System components

Infrastructure

Shopify data processing and storage takes place in North America, in facilities operated by trusted third parties. Shopify uses a combination of colocation facilities for edge routing and public cloud service providers for store hosting and other services.

By default, the infrastructure supporting stores is located in the United States. Shopify also has specialized Canadian infrastructure that is available on request for qualified merchants with strict Canadian localization requirements. In this environment, personally identifiable information (PII) is stored in Canada.

Routing

Default

An incoming web request for an online store hosted by Shopify travels over an encrypted Transmission Control Protocol (TCP) connection to the colocation data centers. The request is then routed to the appropriate region in Shopify's infrastructure, where the message body is decrypted. Information is encrypted in transit using Transport Layer Security (TLS) wherever it passes over the Internet.

Canada

Infrastructure is slightly different for Shopify's Canadian geo-restricted service. Rather than going through routing in the colocation data centers, requests are routed to Shopify's Canadian-hosted infrastructure directly.

Software

The Shopify platform is a multi-tenant cloud-based system that is engineered for high scalability, reliability, and performance. Shopify's software consists of a core application that serves a storefront to customers and potential customers, backed by databases.

The core application makes APIs and dashboards available to store owners and staff to allow them to manage the configuration and business operations of their store in accordance with the features listed in the **Scope** section.

Data

To provide its services, Shopify collects data, primarily from Shopify merchants and merchants' customers. Merchant and customer data is encrypted at rest and sensitive information is further encrypted at the application layer.

Additional information on data collection and usage is noted in Shopify's privacy policy (https://www.shopify.com/legal/privacy).

Control environment

Organizational structure

Shopify maintains an organizational structure and clear lines of responsibility. Shopify's executive team sets the strategic direction for the company and works closely with the senior

leadership team to establish objectives that will allow Shopify to achieve its mission to *Make commerce better for everyone*.

The Shopify Trust team is led by the VP of Security Engineering and IT. This individual is responsible for setting the security direction for the company. The Shopify Trust team's mission is to protect the trust that merchants have placed in Shopify.

In addition to security roles in Trust, other key security and operational roles at Shopify are in the following teams:

- Technology Experience (TX)
- Production Engineering
- Talent
- Legal

Hiring

Role descriptions are published in job postings on the Shopify external careers page (https://www.shopify.com/careers). Potential candidates are evaluated on their ability to meet the position requirements. The interview process includes members of the hiring team and relevant teams based on the position.

Shopify further screens candidates by conducting reference checks before hiring. Contractors who work for an outsourced vendor are screened in accordance with the contract Shopify holds with the vendor.

Board of Directors

The responsibilities of the Board of Directors are outlined in charters that are regularly reviewed by Board members and published on Shopify's website. The Board meets with Shopify's leadership regularly.

Risk assessment

Shopify has defined a risk management process drawn from a mix of standards and industry best practices. The VP of Security Engineering and IT is continuously made aware of security findings, risk decisions, and actions taken. The output of the risk management process is formally communicated to the VP of Security Engineering and IT on a regular basis. This information is communicated to senior management as deemed necessary by the VP of Security Engineering and IT.

Security assessment

Shopify security assessments generate findings that feed the risk management process. Examples of these assessments are:

- Penetration testing
- Vulnerability assessments
- Bug bounty program (https://hackerone.com/shopify)
- Automated vulnerability detection tools
- Security reviews of third-party tools or services
- Trust team assessment of the SOC 2 program

Other operational activities may also generate relevant security findings. These findings along with output from the security assessment are evaluated for risk using the risk management process.

Fraud risk assessment

Shopify conducts a regular fraud risk assessment that identifies and evaluates fraud threats to the organization.

Leadership assessment

Shopify leadership assess adherence to policies, operational irregularities such as availability or security incidents, and regulatory and litigation matters on a regular basis.

Control activities

Policies and procedures

Shopify maintains a security policy that is reviewed regularly and approved by the VP of Security Engineering and IT. Upon hire, Shopify employees are required to review and acknowledge Shopify policies. During employment, Shopify employees are required to review and acknowledge relevant policies regularly. Employees also review and agree to the Code of Conduct regularly.

Shopify maintains security and availability response plans as well as IT Access Provisioning and Deprovisioning procedures, and procedures for reviewing the security of third-party software and services.

Incident management

Shopify believes that security should be a partnership between the company and merchants, which helps the company find security and availability flaws faster and to shorten incident response time. Merchants' customers would report issues to the merchant, who would report them to Shopify.

Shopify's public website (https://www.shopify.com/security-response) instructs merchants on how to report security or availability incidents, how to ask security or availability questions, and how to submit potential security or availability issues. If needed, the Shopify Support team is also available 24/7 to assist merchants with security or availability questions or issues.

If a serious security or availability issue is found, then the incident response process is activated. Incidents are tracked through resolution. When the situation warrants it, Shopify updates the public status page (https://status.shopify.com).

Service monitoring

Shopify maintains the security and availability of systems through automated logging, monitoring, and alerting.

Shopify forwards application and infrastructure logs to a centralized logging service for aggregation, correlation, and alerting. Logs are retained according to a defined retention schedule.

Shopify also monitors production infrastructure metrics.

The logging and monitoring services are configured to generate security alerts. The alerts page an on call team member who evaluates if the alert could represent a security or availability incident. Relevant team members are on call 24/7.

Logical access control

Merchant access

When a merchant creates their Shopify store online, their staff owner account is also created. Store owners can provision staff accounts, which they may set up to have only limited access to their store's data.

There are two main flows for a merchant to authenticate to their account: visiting their store address directly or via https://www.shopify.com. In both workflows, credentials are sent over Hyper Text Transfer Protocol Secure (HTTPS). The Shopify application hashes the password and checks it against the stored hash. Store owners and staff should set up their accounts to use two-factor authentication (2FA) to further secure their accounts.

The store owner's account and all staff accounts are terminated when a merchant closes their store. Merchants may also terminate staff accounts individually through the Shopify admin.

Shopify employee access

Default access

During onboarding, employees are provisioned an email account and an SSO account. Employees must authenticate with SSO to access email. 2FA is enforced on SSO accounts.

Employees access the code base using individual version control system accounts with unique usernames and passwords. Those accounts are invited to the Shopify version control system organization, which associates the version control system account with the user's email. 2FA is required on the version control system account for the invitation to be sent.

Remote access over the Internet is the primary means of default employee access, and authentication takes place using one of the following:

- Single sign-on (SSO) with 2FA
- Individual accounts with 2FA

Authorization for default access for Shopify employees occurs through identity management in Shopify's security systems. Employees belong to groups that define application level permissions. Groups that are assigned to all employees define a set of default applications and capabilities.

Shopify removes employee access promptly following termination and according to a Shopify deprovisioning procedure.

Elevated access

Shopify restricts employee access to the production environment, and internal applications that manage production access, according to the principle of least privilege.

Access to production, or applications that manage production access, is granted through one of the following mechanisms:

- Addition to an access control group

- Configuration management
- Invitation by a security system administrator

Access takes place over the Internet and authentication takes place using one of the following:

- SSO with 2FA
- Individual accounts with 2FA
- Certificate-based authentication

Authorization takes place using, one of:

- Access groups
- Cloud provider identity management
- Operating-system-based account permissions

Account termination for production environments follows the same process as for default access.

Network access

Depending on the environment, network access controls are defined per network:

- Directly in routing devices
- Security groups
- Firewall rules
- Infrastructure ingress resources

Cross environment resource access takes place over TLS.

Internal network controls are governed by:

- Use of private Internet Protocol (IP) addresses
- Application-level access permissions

- AWS firewall rules
- Google Cloud Firewall rules
- GKE network policies

Application and infrastructure change management

Shopify's application and infrastructure change management process follows the principles of test-driven development, using the version control system.

Shopify's Development Handbook defines procedures for reviewing, deploying, and backing out changes. It also includes best practices for coding and security.

Shopify's deploy tooling provides functionality for a developer to initiate an automatic rollback to a previous deploy.

Availability

Shopify manages resources on an ongoing basis.

Shopify maintains a documented project to prepare for high load and component failure scenarios. Systems and procedures relevant to the project are tested and documentation is updated regularly.

Full images of Shopify production databases are backed up and backups are tested regularly.

Shopify's business continuity and disaster recovery planning combines capacity planning with backup recovery verification.

Information and communication

Internal communication

Shopify conducts security training for new employees. The training reinforces the commitments outlined in the security policy.

Shopify's commitments to the security and availability of the system are posted on an internal site. Shopify communicates timely updates to Shopify employees as required on security and availability topics.

External communication

Shopify uses established communication channels to provide updates to merchants about changes that may impact the security and availability of the service.

Merchants are responsible for reviewing email communications as well as proactively reviewing Shopify's Terms of Service, Acceptable Use Policy, Privacy Policy, and website.

If merchants require additional assistance, Shopify maintains a 24/7 customer support operation (https://help.shopify.com/questions).

Shopify's anonymous whistleblower program is available internally and externally and communicated through the Shopify Code of Conduct, and the Shopify Investor Relations website. Any communications to the whistleblower program are automatically sent to the Chair of the Audit Committee and to the Chief Legal Officer.

Monitoring activities

Shopify routinely monitors the performance of internal controls to verify they are appropriate to the current environment. Members of the Trust team regularly review and update control documentation, and ensure automated processes are monitoring the effectiveness of controls.

Incidents are handled by the appropriate individuals, depending on the severity, or potential severity, of the incident. Material incidents are disclosed to the executive team and the Board of Directors.

Subservice organizations

Shopify's subservice organizations include:

- **Amazon Web Services (AWS):** Cloud platform as a service
- **Google Cloud Platform (GCP):** Cloud platform as a service
- **RagingWire:** Colocation data center
- **ServerCentral:** Colocation data center

Shopify’s controls were designed with the assumption that certain controls would be implemented by these subservice organizations. Certain trust services criteria can be met only if the complementary subservice organization controls assumed in the design of Shopify’s controls are suitably designed and operating effectively, along with related controls at these subservice organizations.

Shopify employees have physical access to RagingWire and ServerCentral. Access is removed when no longer needed, and regular reviews are performed to determine if physical access is appropriate.

To manage the quality of services provided by these third parties, Shopify’s Trust team conducts security reviews of the subservice organizations regularly. Reviewers evaluate attestation reports or inquire about relevant security controls with the third party.

Complementary user entity controls

Shopify's Ecommerce Platform System controls were designed with the assumption that certain controls would be implemented by user entities (or "merchants"). This section describes additional controls that merchants should have in operation to complement the controls of Shopify's Ecommerce Platform System. The list of merchant control considerations presented below and those presented with certain specified categories and criteria do not represent a comprehensive set of all the controls that should be employed by merchants. Merchants may be required to implement additional technical or administrative controls to meet their business and legal needs.

Description	Criteria
Merchants are responsible for periodically reviewing the Terms of Service and Acceptable Use Policy web pages to evaluate if there are new or revised security or availability obligations.	CC 2.2, CC 2.3
Merchants are responsible for periodically reviewing the Shopify website to evaluate if there are new or revised security or availability commitments.	CC 2.2, CC 2.3, CC5.3
Merchants are responsible for reviewing communications from Shopify regarding product changes and if necessary taking steps to mitigate the effects of any changes.	CC 2.2, CC 2.3, CC3.4
Merchants are responsible for ensuring that administration access to their stores is restricted to appropriate users and is provisioned in line with corporate policies and requirements.	CC 6.2, CC 6.3
Merchants are responsible for notifying Shopify of any unauthorized use of, and other known or suspected breach of, security related to the system.	CC 6.2, CC 6.3, CC 6.6
Merchants are responsible for ensuring that the contact information associated with their accounts is accurate and kept up to date.	CC 2.1, CC 2.3
Merchants are responsible for ensuring that their passwords are kept confidential.	CC 6.1, CC6.6
Merchants are responsible for ensuring owner and staff accounts have two-factor authentication enabled.	CC 6.6