LIME SECURITY, PRIVACY, AND ARCHITECTURE

Last Updated: September 26, 2016

FinAccel's Corporate Trust Commitment

FinAccel (FinAccel Pte Ltd) is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by customers to our services ("Customer Data").

Services Covered

This documentation is applicable to the services branded as Lime (collectively, the "Lime Services"), provided by FinAccel. This documentation describes the architecture of, the security and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to the Lime Services.

Third-Party Architecture

The architecture used by FinAccel to host Customer Data submitted to the Lime Services is provided by a third-party provider, Amazon Web Services, Inc. ("AWS"). Currently, the architecture hosted by AWS in provisioning of the Lime Services is located in Singapore.

Additionally, a portion of customer support for the Lime Services is provided using third-party technology, being hosted on the third-party's architecture.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the Lime Services:

> GeoTrust SSL Certificates: All Lime Services secure and transmit user data using GeoTrust SSL certificates.

Additionally, the Lime Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis. Information about security and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and Service Organization Control (SOC) reports, is available from the AWS Security Website and the AWS Compliance Website.

Security Controls

The Lime Services include a variety of security controls. These controls include:

Unique user identifiers (user IDs) to ensure that activities can be attributed to the

responsible individual;
Password length controls;

Password complexity requirements for Web and mobile access to the Lime Services; 2 Factor Authentication for transactions made using the Lime Services;

Security Procedures, Policies and Logging

The Lime Services are operated in accordance with the following procedures to enhance security:

User passwords are stored using a salted hash format and are never transmitted

unencrypted;

User access log entries will be maintained, containing date, time, URL executed or entity ID operated on, operation performed (viewed, edited, etc.) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or

PAT (Port Address Translation) is used by a customer or its ISP;

Logs will be stored in a secure centralized host to prevent tampering;
Passwords are not logged under any circumstances;

No defined passwords are set by FinAccel;

Intrusion Detection

FinAccel, or an authorized independent third party, will monitor the Lime Services for unauthorized intrusions using network-based intrusion detection mechanisms. FinAccel may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Lime Services function properly.

Security Logs

All systems used in the provision of the Lime Services log information to their respective system's log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

FinAccel maintains security incident management policies and procedures. FinAccel promptly notifies impacted customers of any actual or reasonably-suspected unauthorized disclosure of their respective Customer Data by FinAccel or its agents of which FinAccel becomes aware to the extent permitted by law.

User Authentication

Access to the Lime Services, directly or via the Lime API, requires a valid user ID and password combination, or an API key/secret, both of which are encrypted via TLS while in transmission. Following a successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security

Production data centers used to provide the Lime Services have systems that control physical access to the data center. These systems permit only authorized personnel to access secure areas. The facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, physical access screening and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure. Further information about physical security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

Reliability and Backup

All networking components, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Lime Services is stored on a primary

database server that is clustered with a backup database server for higher availability. All Customer Data submitted to the Lime Services is backed up daily.

Viruses

The Lime Services do not scan for viruses that could be included in attachments or other data uploaded into the Lime Services by customers.

Data Encryption

The Lime Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Lime Services, including 256-bit TLS Certificates and 256-bit AES encryption at a minimum.

Deletion of Customer Data

Once a user is inactive (no transaction done for at least one year did not activate account for three months), Customer Data will remain in inactive status on back-up media for 90 days, after which it will be overwritten or deleted. This process is subject to applicable legal requirements. Without limiting the ability for customers to request return of their Customer Data submitted to the Lime Services, FinAccel reserves the right to reduce the number of days it retains such data after a user has reached inactive status. FinAccel will update this Lime Security, Privacy, and Architecture Documentation in the event of such a change.

Tracking and Analytics

FinAccel may track and analyze use of the Lime Services for the purposes of security and helping FinAccel improve both the Lime Services and the user experience in using the Lime Services. FinAccel may also use this information and users' e-mail addresses to contact customers or their users to provide information about the Lime Services. Without limiting the foregoing, FinAccel may share data about FinAccel customers' or their users' use of the Lime Services ("Usage Statistics") to FinAccel's service providers for the purpose of helping FinAccel in such tracking or analysis, including improving its users' experience with the Lime Services, or as required by law.

Interoperation with Other FinAccel Services

The Lime Services may interoperate with other services provided by FinAccel.