IBM Security Trusteer Fraud Protection

The Terms of Use ("ToU") is composed of this IBM Terms of Use - SaaS Specific Offering Terms ("SaaS Specific Offering Terms") and a document entitled IBM Terms of Use - General Terms ("General Terms") available at the following URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

In the event of a conflict, the SaaS Specific Offering Terms prevail over the General Terms. By ordering, accessing or using the IBM SaaS, Client agrees to this ToU.

The ToU is governed by the IBM International Passport Advantage Agreement, the IBM International Passport Advantage Express Agreement, or the IBM International Agreement for Selected IBM SaaS Offerings, as applicable ("Agreement") and together with the ToU make the complete agreement.

1. IBM SaaS

The following IBM SaaS offerings are covered by these SaaS Specific Offering Terms:

1.1 Rapport IBM SaaS Offerings

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Pinpoint IBM SaaS Offerings

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Mobile IBM SaaS Offerings

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

2. Charge Metrics

The IBM SaaS is sold under one of the following charge metric(s) as specified in the Transaction Document:

a. Eligible Participant is a unit of measure by which the IBM SaaS can be obtained. Each individual or entity eligible to participate in any service delivery program managed or tracked by the IBM SaaS is an Eligible Participant. Sufficient entitlements must be obtained to cover all Eligible Participants managed or tracked within the IBM SaaS during the measurement period specified in Client's Transaction Document.

   Each service delivery program managed by the IBM SaaS is analyzed separately and then added together. Individuals or entities eligible for multiple service delivery programs require separate entitlements.

   For these offerings, a service delivery program includes a single Business or Retail Application of the Client with a main login page and related pages for each Business or Retail Application. An Eligible Participant is an end user of a Client, who has login credentials on the Business or Retail Application.

b. Client Device is a unit of measure by which the IBM SaaS can be obtained. A Client Device is a single user computing device or special purpose sensor or telemetry device that requests the execution of or receives for execution a set of commands, procedures, or applications from or provides data to another computer system that is typically referred to as a server or is otherwise managed by the server. Multiple Client Devices may share access to a common server. A Client Device may have some processing capability or be programmable to allow a user to do work. Client must obtain entitlements for every Client Device which runs, provides data to, uses services provided by, or otherwise accesses the IBM SaaS during the measurement period specified in Client's Transaction Document.

3. Charges and Billing

The amount payable for the IBM SaaS is specified in a Transaction Document.

3.1 Partial Month Charges

A partial month charge as specified in the Transaction Document may be assessed on a pro-rated basis.

4. Compliance and Auditing

Access to the IBM Security Trusteer Fraud Protection offerings is subject to a maximum quantity of Eligible Participants or Client Devices as specified in the Transaction Document. Client is responsible for ensuring that their number of Eligible Participants or Client Devices does not exceed the maximum quantity as specified in the Transaction Document.

An audit may be conducted to verify compliance with maximum quantity of Eligible Participants or Client Devices.

5. IBM SaaS Subscription Period Renewal Options

Client's Transaction Document will set forth whether the IBM SaaS will renew at the end of the Subscription Period, by designating one of the following:

5.1 Automatic Renewal

If Client's Transaction Document states that Client's renewal is automatic, Client may terminate the expiring IBM SaaS Subscription Period by written request to Client's IBM sales representative or IBM Business Partner, at least ninety (90) days prior to the expiration date as set forth in the Transaction Document. If IBM or its IBM Business Partner does not receive such termination notice by the expiration date, the expiring Subscription Period will be automatically renewed for either one year or the same duration as the original Subscription Period as set forth in the Transaction Document.

5.2 Continuous Billing

When the Transaction Document states that Client's renewal is continuous, Client will continue to have access to the IBM SaaS and will be billed for the usage of the IBM SaaS on a continuous basis. To discontinue use of the IBM SaaS and stop the continuous billing process, Client will need to provide IBM or its IBM Business Partner with ninety (90) days written notice requesting that Client's IBM SaaS be cancelled. Upon cancellation of Client's access, Client will be billed for any outstanding access charges through the month in which the cancellation took effect.

5.3 Renewal Required

When the Transaction Document states that Client's renewal type is "terminate", the IBM SaaS will terminate at the end of the Subscription Period and Client's access to the IBM SaaS will be removed. To continue to use the IBM SaaS beyond the end date, Client will need to place an order with Client's IBM sales representative or IBM Business Partner to purchase a new Subscription Period.

6. Technical Support

Technical Support for the IBM SaaS is available to a Client and their Eligible Participants to assist in their use of the IBM SaaS.

Standard Support is included in the subscription of all offerings. Trusteer Rapport Mandatory Service, which is an add-on to Trusteer Rapport, has a prerequisite of Premium Support for the base Trusteer Rapport subscription.

For each IBM SaaS offering, a Premium Support subscription is available for an additional charge, with the exception of IBM Security Trusteer Mobile SDK offerings and IBM Security Trusteer Rapport Mandatory Service offerings.

Standard Support:

- 8AM-5PM local time support.
- Clients and their Eligible Participants can submit support tickets electronically, as detailed in the Software as a Service [SaaS] Support Handbook.
- Clients can access Client Support Portal for notifications, documents, case reports and FAQs at: http://www-01.ibm.com/software/security/trusteer/support/.
- For support options and details access the IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

Premium Support:

- 24x7 support for all severities.
- Clients can reach support directly via phone.
- Clients and their Eligible Participants can submit support tickets electronically, as detailed in the Software as a Service [SaaS] Support Handbook.
- Clients can access Client Support Portal for notifications, documents, case reports and FAQs at: http://www-01.ibm.com/software/security/trusteer/support/.
- For support options and details access the IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

7. IBM SaaS Offering Additional Terms

7.1 Safe Harbor Compliance

IBM adheres to the U.S.-EU Safe Harbor Framework developed by the U.S. Department of Commerce in coordination with the European Commission. IBM Security Trusteer products are included in IBM's EU-U.S. Safe Harbor certification. More information on Safe Harbor and the Safe Harbor company list can be found here:

http://export.gov/safeharbor/

7.2 Client Annual Subscription Fee Increase

IBM reserves the right to adjust the subscription fee for the IBM SaaS no more than once every twelve (12) months by a percentage to be determined by IBM not to exceed 3%. The subscription fee adjustment will be effective on the anniversary of the initial starting coverage period date. This fee adjustment does not alter Client's entitlement to the IBM SaaS or the charge metric by which the IBM SaaS is obtained. IBM Business Partners are independent from IBM and unilaterally determine their prices and terms.

7.3 Premium Support

Client is entitled to Premium Support only for IBM SaaS offerings for which Client has subscribed to the associated Premium Support offering.

7.4 Lawful Use and Consent

Authorization to Collect and Process Data

The IBM SaaS is designed to help Client improve its security environment and data. The IBM SaaS will collect information from Eligible Participants and Client Devices who interact with the Business or Retail Applications for which Client has subscribed to IBM SaaS offerings coverage. The IBM SaaS collects information that alone or in combination may be considered Personal Data in some jurisdictions. Personal Data is any information that can be used to identify a specific individual, such as a name, email address, home address, or phone number that is provided to IBM to store, process, or transfer on Client's behalf.

Data collection and processing practices may be updated to improve the functionality of the IBM SaaS. A document with a full description of the data collection and processing practices is updated as needed and is available to Client upon request. Client authorizes IBM to collect this information and process it in accordance with the Cross Border Transfers section and the Data Privacy section of this ToU, and the Data Privacy and Data Security section of the ToU General Terms.

For IBM Security Trusteer Pinpoint offerings:

Collected data may include user IP address, encrypted or one-way hashed user ID, domain cookies if not filtered, visits to protected Applications and phishing sites, geographical location, and credentials entered into phishing sites.

For IBM Security Trusteer Mobile SDK offerings and IBM Security Trusteer Mobile Browser offerings:

Collected data may include user IP address, encrypted or one-way hashed user ID, geographical location, and visits to protected Applications, SIM card information, device name, and client affiliation.

For IBM Security Trusteer Rapport offerings:

Collected data may include user IP address, encrypted or one-way hashed user ID, security events, user name and email address provided for the purpose of contacting IBM for Client support, client affiliation, encrypted password entered on protected sites, visits to protected Applications and phishing sites, encrypted payment card number, and files and data collected remotely by IBM personnel to inspect suspected malware, malicious activity, or malfunction.

Informed Consent from Data Subjects

Use of this IBM SaaS may implicate various laws or regulations. The IBM SaaS may be used only for lawful purposes and in a lawful manner. Client agrees to use the IBM SaaS pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies.

For IBM Security Trusteer Pinpoint offerings and for IBM Security Trusteer Mobile SDK offerings:

Client agrees that it has obtained or will obtain any fully informed consents, permissions, or licenses necessary to enable lawful use of the IBM SaaS and to permit collection and processing of the information by IBM through the IBM SaaS.

For IBM Security Trusteer Rapport offerings and for & IBM Security Trusteer Mobile Browser offerings:

Client authorizes IBM to obtain fully informed consents necessary to enable lawful use of the IBM SaaS and to collect and process the information as described in the End User License Agreement available at https://www.trusteer.com/support/end-user-license-agreement. In the event Client determines that it (and not IBM) will handle consent communications with end users, Client agrees that it has obtained or will obtain any fully informed consents, permissions, or licenses necessary to enable lawful use of the IBM SaaS and to permit collection and processing of the information by IBM as Client's data processor through the IBM SaaS.

7.5 Cross Border Transfers

Client agrees that IBM may process the content, including any Personal Data, under relevant laws and requirements across a country border to processors and sub-processors in the following countries outside of the European Economic Area and countries considered by the European Commission to have adequate levels of security: the USA.

7.6 Data Privacy

If Client makes Personal Data available to IBM SaaS in the EU Member States, Iceland, Liechtenstein, Norway, or Switzerland, or if Client has Eligible Participants or Client Devices in those countries, then Client as the sole controller appoints IBM as a processor to process (as those terms are defined in EU Directive 95/46/EC) Personal Data. IBM will only process such Personal Data to the extent required to make the IBM SaaS offering available in accordance with IBM's published descriptions of IBM SaaS and Client agrees that any such processing is in accordance with Client's instructions. IBM will provide reasonable advance notice if IBM makes a material change to the processing location or the way it secures Personal Data as part of IBM SaaS. Client may terminate the current Subscription Period for the affected IBM SaaS, by providing written notice to IBM within thirty (30) days of IBM's notification of the change to Client. Client agrees that IBM may process content including any Personal Data across a country border to the following processors and sub-processors:

Name of Processor/Sub-processor	Role (Data Processor or Sub-processor)	Location*
The IBM contracting entity	Processor	As stated on the Transaction Document
Amazon Web Services LLC	Sub-processor	410 Terry Ave. N Seattle, WA 98109 United States
Connectria Corp.	Sub-processor	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 United States
IBM Israel Ltd.	Sub-processor	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel
IBM Corp	Sub-processor	1 New Orchard Rd. Armonk, NY 10504 United States

Client agrees that IBM may, on notice, vary this list of country locations when it reasonably determines it necessary for the provision of the IBM SaaS.

Client agrees that for service provided through the German data center, as determined during the provisioning process, IBM may process content including any Personal Data across a country border to the following processors and sub-processors:

Name of Processor/Sub-processor	Role (Data Processor or Sub-processor)	Location*
The IBM contracting entity	Processor	As stated on the Transaction Document

Amazon Web Services (Germany)	Sub-processor	Munich, Germany
IBM Israel Ltd.	Sub-processor	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

Client agrees that for service provided through the Japan data center, as determined during the provisioning process, IBM may process content including any Personal Data across a country border to the following processors and sub-processors:

Name of Processor/Sub-processor	**Role (Data Processor or Sub-processor)**	**Location***
The IBM contracting entity	Processor	As stated on the Transaction Document
Amazon Web Services (Japan)	Sub-processor	Tokyo, Japan
IBM Israel Ltd.	Sub-processor	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

* The locations identified in the tables above include the addresses of the corporate offices of the Processor/Sub-processor. The data centers are located within the same country identified.

The parties or their relevant affiliates may enter into separate standard unmodified EU Model Clause agreements in their corresponding roles pursuant to EC Decision 2010/87/EU with optional clauses removed. All disputes or liability arising under these agreements, even if entered into by affiliates, will be treated by the parties as if the dispute or liability arose between them under the terms of this Agreement.

Appendix A

1. IBM SaaS Offerings

IBM offers these services as stand alone services and offerings, or as additional services and offerings. The specific IBM SaaS offerings ordered are specified in Client's PoE.

1.1 Business and Retail Definitions

The IBM Security Trusteer fraud products are licensed for use with specific types of Applications. An Application is defined as one of the following types: Retail or Business. Separate offerings are available for Retail Applications and Business Applications.

- A Retail Application is defined as an online banking application, mobile application or e-commerce application designed to service consumers. Client policy may classify certain small businesses as eligible for retail access.
- A Business Application is defined as an online banking application, mobile application or e-commerce application designed to service corporate, institutional, or equivalent entities, or any application that is not categorized as Retail.

1.2 IBM SaaS Base Subscription Offerings

Business Offerings:

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

Retail Offerings:

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

For each of the Business and Retail offerings, there is an associated Premium Support product available for an additional charge, with the exception of the IBM Security Trusteer Mobile SDK offerings.

1.3 Additional IBM SaaS Subscription Offerings for IBM Security Trusteer Rapport Offerings

Additional offerings available for IBM Security Trusteer Rapport for Business:

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

Additional offerings available for IBM Security Trusteer Rapport for Retail:

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

For each of the Business and Retail add-ons to the IBM Security Trusteer Rapport offerings, except for the IBM Security Trusteer Rapport Mandatory Service add-ons, there is an associated Premium Support product available for an additional charge.

Subscription to IBM Security Trusteer Rapport for Business or IBM Security Trusteer Rapport for Retail is a prerequisite to the associated additional IBM SaaS subscription offerings listed in this section.

1.4 Additional IBM SaaS Subscription Offerings for IBM Security Trusteer Pinpoint Malware Detection Offerings

Additional offerings available for IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition or IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Additional offerings available for IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition or IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

Premium Support subscription is available for an additional charge for each of the additional IBM SaaS offerings listed in this section.

Subscription to IBM Security Trusteer Pinpoint Malware Detection for Business offerings or IBM Security Trusteer Pinpoint Malware Detection for Retail offerings is a prerequisite to the associated additional IBM SaaS subscription offerings listed in this section.

1.5 Other Additional IBM SaaS Subscriptions

Any additional IBM SaaS Subscription for the base subscriptions above that is not listed herein, either currently available or under development, is not considered an update and must be granted separately.

1.6 Definitions

"Account Holder" means the end user of the Client, who has installed the client-enabling software, accepted the end user license agreement ("EULA"), and authenticated at least once with the Client's Retail or Business Application for which Client has subscribed to IBM SaaS offerings coverage.

"Account Holder Client Software" means the IBM Security Trusteer Rapport client-enabling software or the IBM Security Trusteer Mobile Browser client-enabling software or the any other client-enabling software that is provided with some IBM SaaS subscriptions for installation on the end user's device.

"Trusteer Splash" refers to the splash that is provided to the Client based on available splash templates.

"Landing Page" refers to the IBM-hosted page that is provided to the Client with Client splash and downloadable Account Holder Client Software.

2. IBM Security Trusteer Rapport Offerings

2.1 IBM Security Trusteer Rapport for Retail and/or IBM Security Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport provides a layer of protection against phishing and Man-in-the-Browser (MitB) malware attacks. Using a network of tens of millions of endpoints across the globe, IBM Security Trusteer Rapport collects intelligence on active phishing and malware attacks against organizations worldwide. IBM Security Trusteer Rapport applies behavioral algorithms aimed to block phishing attacks and to prevent the installation and the operation of MitB malware strains.

This IBM SaaS offering has an Eligible Participant charge metric. The Business offering is sold in packs of 10 Eligible Participants. The Retail offering is sold in packs of 100 Eligible Participants.

This IBM SaaS offering includes:

a. Trusteer Management Application ("TMA"):

   The TMA is made available on the IBM Security Trusteer cloud-hosted environment, through which the Client (and unlimited number of its authorized personnel) can: (i) receive event data reporting and risk assessments, (ii) view, configure, and set policies relating to reporting of the events data, and (iii) view the configuration of the client-enabling software licensed to the public under an end user license agreement ("EULA") at no charge, and made available to download onto Eligible Participant's desktops or devices (PC/MACs), also known as Trusteer Rapport software suite

("Account Holder Client Software"). Client may only market the Account Holder Client Software using the Trusteer Splash or Rapport API, and Client may not use the Account Holder Client Software for its internal business operations or for its employees' use (other than employees' personal use).

b. Web Script:

For access on a website for the purposes of accessing or using the IBM SaaS offerings.

c. Events data:

The Client (and unlimited number of its authorized personnel) can use the TMA to receive events data generated from Account Holder Client Software as a result of Account Holders' online interactions with its Business or Retail Application for which Client has subscribed to IBM SaaS offerings coverage. Events data will be received from the Eligible Participants' Account Holder Client Software that is running on their devices, who have accepted the EULA, authenticated with the Client's Business or Retail Application at least once, and Client's configuration must include collection of User IDs.

d. Trusteer Splash:

The Trusteer Splash marketing platform identifies and markets the Account Holder Client Software to the Eligible Participants accessing Client's Business and/or Retail Applications for which Client has subscribed to IBM SaaS offerings coverage. The Client may select from available Splash Templates. Customized splash may be contracted under a separate agreement or statement of work.

Client may agree to provide its trademarks, logos or icons for use in connection with the TMA and only for utilization with the Trusteer Splash and for display in the Account Holder Client Software or on the landing pages hosted by IBM and on the IBM Security Trusteer website. Any use of its provided trademarks, logos, or icons will be in accordance with IBM's reasonable policies regarding advertising and trademark usage.

Client must subscribe to the IBM Security Trusteer Rapport Mandatory Service SaaS offering if Client wishes to employ any type of mandatory deployment of the Account Holder Client Software.

Mandatory deployment of the Account Holder Client Software includes but is not limited to, any type of mandatory deployment by any mechanism or means which directly or indirectly compels an Eligible Participant to download the Account Holder Client Software, or any method, tool, procedure, agreement or mechanism, not created by or approved by IBM, created to bypass the licensing requirements of this mandatory deployment of the Account Holder Client Software.

2.2 Optional Additional IBM SaaS Offerings for IBM Security Trusteer Rapport for Business and/or IBM Security Trusteer Rapport for Retail

Subscription to IBM Security Trusteer Rapport offerings is a perquisite to subscription to any of the following additional IBM SaaS offerings. If the IBM SaaS is designated as "for Business", then the additional IBM SaaS offering acquired must also be designated as "for Business". If the IBM SaaS is designated as "for Retail", then the additional IBM SaaS offering acquired must also be designated as "for Retail". Client will receive events data from Eligible Participants running the Account Holder Client Software who have accepted the EULA, authenticated with Client's Business and/or Retail Application(s) at least once, and Client's configuration must include collection of User IDs.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business and/or IBM Security Trusteer Rapport Fraud Feeds for Retail

Client (and unlimited number of its authorized personnel) can use the TMA to receive events data relating to malware infections and other endpoint vulnerabilities on a particular Account Holder's desktop.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business and/or IBM Security Trusteer Rapport Phishing Protection for Retail

Client (and unlimited number of its authorized personnel) can use the TMA to receive events data notifications relating to submission of Account Holder's login credentials to a suspected phishing or potentially fraudulent site. Legitimate online applications (URLs) may erroneously be flagged as phishing sites and the IBM SaaS may alert Account Holders that a legitimate site is a phishing site. In such event, Client must notify IBM of such error, and IBM shall correct the error. This shall be Client's sole remedy for such error.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business and/or IBM Security Trusteer Rapport Mandatory Service for Retail

Client may use an instance of the Trusteer Splash marketing platform to mandate the download of the Account Holder Client Software to Eligible Participants accessing Client's Business and/or Retail Applications for which Client has subscribed to IBM SaaS offerings coverage.

IBM Security Trusteer Rapport Premium Support for Business is a prerequisite to IBM Security Rapport Mandatory Service for Business.

IBM Security Trusteer Rapport Premium Support for Retail is a prerequisite to IBM Security Rapport Mandatory Service for Retail.

Client may implement the IBM Security Trusteer Rapport Mandatory Service additional functionality only if it was ordered and configured for use with Client's Retail or Business Application for which Client has subscribed to IBM SaaS offerings coverage.

3. IBM Security Trusteer Pinpoint Offerings

IBM Security Trusteer Pinpoint is a cloud-based service that is designed to provide another layer of protection and aims to detect and mitigate malware, phishing and account takeover attacks. Trusteer Pinpoint can be integrated into Client's Business and/or Retail Applications for which Client has subscribed to IBM SaaS offerings coverage and fraud prevention processes.

This IBM SaaS offering includes:

a. TMA:

The TMA is made available on the IBM Security Trusteer cloud-hosted environment, through which Client (and unlimited number of authorized personnel) can: (i) receive event data reporting and risk assessments, and (ii) view, configure, and set security policies and policies relating to reporting of the events data.

b. Web Script and/or APIs:

For deployment on a website for the purposes of accessing or using the IBM SaaS.

3.1 IBM Security Trusteer Pinpoint Malware Detection and IBM Security Trusteer Pinpoint Criminal Detection

In the event of malware detection in IBM Security Trusteer Pinpoint Malware Detection offerings or account takeover detection in IBM Security Trusteer Pinpoint Criminal Detection offerings, Client must follow the Pinpoint Best Practices Guide. Do not use IBM Security Trusteer Pinpoint Malware Detection offerings or IBM Security Trusteer Pinpoint Criminal Detection offerings in any way that will affect the Eligible Participant's experience immediately after a malware or account takeover detection, such that it would enable others to link Client's actions with the use of IBM Security Trusteer Pinpoint offerings (e.g., notifications, messages, blocking of devices, or blocking of access to the Business and/or Retail Application immediately after a malware or account takeover detection).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business and/or IBM Security Trusteer Pinpoint Criminal Detection for Retail

Clientless detection of a suspicious account takeover activity of browsers connecting to a Business or Retail Application, using device ID, phishing detection, and malware-driven credential theft detection. IBM Security Trusteer Pinpoint Criminal Detection offerings provide another layer of protection and aim to detect account takeover attempts and deliver risk assessment scores of browsers or mobile devices (through the native browser or the Client mobile application) accessing a Business or Retail Application directly to Client.

a. Events data:

Client (and unlimited number of its authorized personnel) can use the TMA to receive events data generated as a result of Eligible Participants' online interactions with Client's Business and/or Retail Application(s) for which Client has subscribed to IBM SaaS offerings coverage or Client can receive the events data via a backend API delivery mode.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile and/or IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) offerings are designed to provide another layer of protection and aim to protect against account takeover and fraudulent activities

by identifying criminal account access and by providing a recommendation to Client. This IBM SaaS offering collects information coming both from Client's Business and/or Retail Application using the PPCD Mobile API, and from mobile devices of Eligible Participants. IBM Security Trusteer PPCD Mobile offerings are designed to correlate complex information related to mobile devices of Eligible Participants with other data sources, such as real-time malware infection and phishing incidents that are integrated via IBM Security Trusteer's other IBM SaaS offerings specified in this ToU.

Client can access and use the IBM Security Trusteer PPCD Mobile offerings on IBM Security Trusteer's cloud-hosted environment and receive risk assessments data from mobile devices of Eligible Participants, generated as a result of the online interactions of these mobile devices with the Client's Business or Retail Application for which Client has subscribed to IBM SaaS offerings coverage. For purpose of these offerings, "mobile devices" include only supported mobile phones and tablets and do not include PCs or MACs.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition and/or IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition and/or IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition and/or IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Clientless detection of Man in the Browser (MitB) financial malware-infected browsers connecting to a Business and/or Retail Application. IBM Security Trusteer Pinpoint Malware Detection offerings provide another layer of protection and aim to enable organizations to focus on fraud prevention processes based on malware risk by providing Client with assessments and alerts of a presence of MitB financial malware.

a. Events data:

   Client (and unlimited number of its authorized personnel) can use the TMA to receive events data generated as a result of Eligible Participants' online interactions with Client's Business and/or Retail Application(s).

b. Advanced Edition:

   The Advanced Editions for Business and/or for Retail offers an additional layer of detection and protection that is adjusted and customized to the Client's Business and/or Retail Applications' structure and flow, and can be customized to the specific threat landscape targeting the Client. It can be incorporated in various locations in the Client's Business and/or Retail Applications.

   The Advanced Edition is offered to Client at minimum quantities of at least 100K Retail Eligible Participants or 10K Business Eligible Participants, which is 1000 packs of 100 Eligible Participants for Retail, or 1000 packs of 10 Eligible Participants for Business.

c. Standard Edition:

   The Standard Edition for Business or for Retail is a fast-to-deploy solution that provides the core functionality of this IBM SaaS offering as described herein.

3.2 Optional Additional IBM SaaS Offerings for IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition and/or IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition and/or IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition and/or IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

For the IBM Security Trusteer Rapport Remediation for Retail offerings, there is a prerequisite of IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition or IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition.

For IBM Security Trusteer Pinpoint Carbon Copy for Retail, there is a prerequisite of IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition or IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition. For IBM Security Trusteer Pinpoint Carbon Copy for Business, there is a prerequisite of IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition or IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business and/or IBM Security Trusteer Pinpoint Carbon Copy for Retail

IBM Security Trusteer Pinpoint Carbon Copy offerings designed to provide another layer of protection and a monitoring service that can help identify when an Eligible Participant's credentials have been

compromised by Phishing attacks on Client's Retail or Business Applications for which Client has subscribed to IBM SaaS offerings coverage.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail aims to investigate, remediate, block and remove man-in-the-browser (MitB) malware infections from infected devices (PC/MACs) of Client's Eligible Participants who access the Client's Retail Application on an ad-hoc basis, where MitB malware infections have been detected by IBM Security Trusteer Pinpoint Malware Detection events data. Client must have current subscription to IBM Security Trusteer Pinpoint Malware Detection actually running on Client's Retail Application. Client may use this IBM SaaS offering only in connection with Eligible Participants who access the Client's Retail Application, and solely as tool that aims to investigate and remediate a particular infected device (PC/MAC) on an ad-hoc basis. The IBM Security Trusteer Rapport Remediation for Retail must actually run on such affected Eligible Participant's device (PC/MAC), and such affected Eligible Participant has to accept the EULA, authenticate with Client's Retail Application(s) at least once, and Client's configuration must include collection of User IDs. For avoidance of doubt, this IBM SaaS offering does not include the right to use the Trusteer Splash and/or promote the Account Holder Client Software in any other way to the Client's general Eligible Participants population.

4. IBM Security Trusteer Mobile Offerings

4.1 IBM Security Trusteer Mobile Browser for Business and/or IBM Security Trusteer Mobile Browser for Retail

IBM Security Trusteer Mobile Browser is designed to add another layer of protection and aims to provide safe online access of Eligible Participants' mobile devices accessing Client's Retail or Business Applications for which Client has subscribed to IBM SaaS offerings coverage, mobile devices' risk assessment, and phishing protection. Secure Wi-Fi detection is only available for Android platforms. For the purpose of this IBM SaaS offering include mobile devices include mobile phones or tablets and do not include Laptop PCs and Macs.

Through the TMA, Client (and unlimited number of its authorized personnel) may receive events data, analysis, and statistics information relating to Devices whose Eligible Participants have: (i) downloaded the Account Holder Client Software, an application licensed to the public under an end user license agreement ("EULA") at no charge, and made available to download onto Eligible Participants' mobile devices, and (ii) accepted the EULA and authenticated at least once with Client's Business or Retail Applications for which Client has subscribed to IBM SaaS offerings coverage. Client may only market the Account Holder Client Software using Trusteer Splash and may not use the Account Holder Client Software for its internal business operations.

a. Events data:

   Client (and unlimited number of its authorized personnel) may use the TMA to receive events data generated as a result of the mobile devices online interactions with Client's Retail or Business Applications for which Client has subscribed to IBM SaaS offerings coverage.

b. Trusteer Splash:

   The Trusteer Splash marketing platform identifies and markets the Account Holder Client Software to the Eligible Participants accessing Client's Business and/or Retail Applications for which Client has subscribed to IBM SaaS offerings coverage. The Client may select from available splash templates ("Splash Template"). Customized splash may be contracted under a separate agreement or statement of work.

Client may agree to provide its trademarks, logos or icons for use in connection with the TMA and only for utilization with the Trusteer Splash and for display in the Account Holder Client Software or on the landing pages hosted by IBM or on the IBM Security Trusteer website. Any use of its provided trademarks, logos, or icons will be in accordance with IBM's reasonable policies regarding advertising and trademark usage.

4.2 IBM Security Trusteer Mobile SDK for Business and/or IBM Security Trusteer Mobile SDK for Retail

IBM Security Trusteer Mobile SDK offerings are designed to add another layer of protection to provide safe web access onto Client's Business and/or Retail Applications for which Client has subscribed to IBM SaaS offerings coverage, devices' risk assessment, and pharming protection. Secure Wi-Fi detection is only available for Android platforms.

IBM Security Trusteer Mobile SDK offerings include a proprietary mobile software developer's kit ("SDK"), a software package containing documentation, programming proprietary software libraries and other related files and items, known as IBM Security Trusteer mobile library as well as the "Run-time Component," or "Redistributable", a proprietary code generated by the IBM Security Trusteer Mobile SDK that can be embedded and integrated into Client's protected standalone iOS or Android mobile applications for which Client has subscribed to IBM SaaS offerings coverage.("Client Integrated Mobile App").

IBM Security Trusteer Mobile SDK for Retail is available in packs of 100 Eligible Participants or packs of 100 Client Devices, and IBM Security Trusteer Mobile SDK for Business is available in packs of 10 Eligible Participants or packs of 10 Client Devices.

Through the TMA, the Client (and unlimited number of its authorized personnel) may receive event data reporting and risk trends assessments. Through the Client Integrated Mobile App, Client can receive risk analysis and mobile device information relating to mobile devices of the Eligible Participants who have downloaded the Client Integrated Mobile App, allowing the Client to formulate a fraud preventive policy enforcing mitigation actions toward these risks.. For purpose of this offering, "mobile devices" include only supported mobile phones and tablets and do not include PCs or MACs.

Client can:

a. internally use the IBM Security Trusteer Mobile SDK solely for the purpose of developing Client Integrated Mobile App;

b. embed the Redistributable (solely in object code format), as an integral, non-separable way in Client Integrated Mobile App. Any modified or merged portion of Redistributable pursuant to this license grant shall be subject to the terms of this ToU; and

c. market and distribute the Redistributable for download onto mobile devices of Eligible Participants or onto Client Device holder, provided that:

- Except as expressly permitted in this Agreement, Client (1) may not use, copy, modify, or distribute the SDK; (2) may not reverse assemble, reverse compile, or otherwise translate, or reverse engineer the SDK, except as expressly permitted by law without the possibility of contractual waiver; (3) may not sublicense, rent, or lease the SDK; (4) may not remove any copyright or notice files contained in the Redistributable; (5) may not use the same path name as the original Redistributable files/modules; and (6) may not use IBM's, its licensors' or distributors' names or trademarks in connection with the marketing of the Client Integrated Mobile App without IBM's or that licensor's or distributor's prior written consent.
- The Redistributable must remain integrated in a non-separable way within the Client Integrated Mobile App. The Redistributable must be in object code form only and must conform to all directions, instruction and specifications in the SDK and its documentation. The end user license agreement for the Client Integrated Mobile App must notify the end user that the Redistributable may not be i) used for any purpose other than to enable the Client Integrated Mobile App ii) copied (except for backup purposes), iii) further distributed or transferred iv) reverse assembled, reverse compiled, or otherwise translated except as specifically permitted by law and without the possibility of a contractual waiver. Client's license agreement must be at least as protective of IBM as the terms of this Agreement
- The SDK may only be deployed as part of Client's internal development and unit testing on Client's specified mobile testing devices. Client is not authorized to use the SDK for processing production workloads, simulating production workloads or testing scalability of any code, application or system. Client is not authorized to use any part of the SDK for any other purposes.

Client is responsible for all technical assistance for Client Integrated Mobile App and for any modifications to the Redistributables made by Client, as permitted herein.

Client is authorized to install and use the Redistributables and the IBM Security Mobile SDK only to support Client's use of the IBM SaaS offering.

IBM has tested sample applications created with the mobile tools provided in the IBM Security Trusteer Mobile SDK ("Mobile Tools") to determine if they will execute properly on certain versions of mobile operating system platforms from Apple (iOS), Google (Android), and others (collectively "Mobile OS Platforms"), however, Mobile OS Platforms are provided by third parties, are not under IBM's control and are subject to change without notice to IBM. As such, and notwithstanding anything to the contrary, IBM

does not warrant that any applications or other output created using the Mobile Tools will execute properly on, interoperate with or be compatible with any Mobile OS Platforms or mobile devices.

Client agrees to create, retain, and provide to IBM and its auditors accurate written records, system tool outputs, and other system information sufficient to provide auditable verification that Client's use of the IBM Security Trusteer Mobile SDK is in compliance with terms of this ToU.

5. Deployment of IBM SaaS Fraud Protection Offerings

Client's base subscription includes required setup and initial deployment activities, including initial one-time startup, configuration, Splash Template, testing and training.

Additional services may be contracted for an additional charge under a separate agreement.

Appendix B

IBM provides the following availability service level agreement ("SLA") for the IBM SaaS and is applicable if specified in Client's Transaction Document:

The version of this SLA that is current at the commencement or renewal of the term of Client's subscription will apply. Client understands that the SLA does not constitute a warranty to Client.

1. Definitions

a. "Authorized Contact" means the individual Client has specified to IBM who is authorized to submit Claims under this SLA.

b. "Availability Credit" means the remedy IBM will provide for a validated Claim. The Availability Credit will be applied in the form of a credit or discount against a future invoice of subscription charges for the IBM SaaS.

c. "Claim" means a claim submitted by Client's Authorized Contact to IBM pursuant to this SLA that a Service Level has not been met during a Contracted Month.

d. "Contracted Month" means each full month during the term of the IBM SaaS measured from 12:00 a.m. GMT on the first day of the month through 11:59 p.m. GMT on the last day of the month.

e. "Client" means an entity that is subscribing for the IBM SaaS directly from IBM, and that is not in default of any material obligations, including payment obligations, under its contract with IBM for the IBM SaaS.

f. "Downtime" means a period of time during which production system processing for the Service has stopped and all of your users are unable to use all aspects of the Service for which they have appropriate permissions. Downtime does not include the period of time when the Service is not available as a result of:

- Planned System Downtime;
- Force Majeure;
- Problems with Client or third party applications, equipment, or data;
- Client or third party acts or omissions (including anyone gaining access to the IBM SaaS by means of Client's passwords or equipment);
- Failure to adhere to required system configurations and supported platforms for accessing the IBM SaaS; or
- IBM's compliance with any designs, specifications, or instructions provided by Client or a third party on Client's behalf.

g. "Event" means a circumstance or set of circumstances taken together, resulting in a failure to meet a Service Level.

h. "Force Majeure" means acts of God, terrorism, labor action, fire, flood, earthquake, riot, war, governmental acts, orders or restrictions, viruses, denial of service attacks and other malicious conduct, utility and network connectivity failures, or any other cause of the IBM SaaS unavailability that was outside IBM's reasonable control.

i. "Planned System Downtime" means a scheduled outage of the IBM SaaS for the purpose of maintenance.

j. "Service Level" means the standard set forth below by which IBM measures the level of service it provides in this SLA.

2. Availability Credits

a. In order to be eligible to submit a Claim Client must have logged a support ticket for each Event with the IBM client support help desk for the applicable IBM SaaS, in accordance with IBM procedure for reporting Severity 1 support issues. Client must provide all necessary detailed information about the Event and reasonably assist IBM with the diagnosis and resolution of the Event to the extent

required for Severity 1 support tickets. Such ticket must be logged within twenty-four (24) hours of Client's first becoming aware that the Event has impacted Client's use of the IBM SaaS.

b. Client's Authorized Contact must submit Client's Claim for an Availability Credit no later than three (3) business days after the end of the Contracted Month that is the subject of the Claim.

c. Client's Authorized Contact must provide to IBM all reasonable details regarding the Claim, including but not limited to, detailed descriptions of all relevant Events and the Service Level claimed not to have been met.

d. IBM will measure internally total combined Downtime during each Contracted Month applicable to the corresponding Service Level shown on the table below. Availability Credits will be based on the duration of the Downtime measured from the time Client reports that Client were first impacted by the Downtime. If Client reports an Event of Application Downtime and an Event of Inbound Data Processing Downtime occurring simultaneously, then IBM will treat the overlapping periods of Downtime as a single period of Downtime, and not as two separate periods of Downtime. For each valid Claim, IBM will apply the highest applicable Availability Credit based on the achieved Service Level during each Contracted Month, as shown on the tables below. IBM will not be liable for multiple Availability Credits for the same Event(s) in the same Contracted Month.

e. For Bundled Service (individual IBM SaaS packaged and sold together for a single combined price), the Availability Credit will be calculated based on the single combined monthly price for the Bundled Service, and not the monthly subscription fee for each individual IBM SaaS. Client may only submit Claims relating to one individual IBM SaaS in a bundle in any Contracted Month, and IBM will not be liable for Availability Credits with respect to more than one IBM SaaS in a bundle in any Contracted Month.

f. If Client purchased the IBM SaaS from a valid IBM reseller in a remarketing transaction in which IBM maintains primary responsibility for fulfilling the IBM SaaS and SLA commitments, then the Availability Credit will be based on the then-current Relationship Suggested Value Price (RSVP) for the IBM SaaS in effect for the Contracted Month which is the subject of a Claim, discounted at a rate of 50%.

g. The total Availability Credits awarded with respect to any Contracted Month shall not, under any circumstance, exceed ten percent (10%) of one twelfth (1/12th) of the annual charge paid by Client to IBM for the IBM SaaS.

h. IBM will use its reasonable judgment to validate Claims based on information available in IBM's records, which will prevail in the event of a conflict with data in Client's records.

i. THE AVAILABILITY CREDITS PROVIDED TO CLIENT IN ACCORDANCE WITH THIS SLA ARE CLIENT'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM.

3. Service Levels

Availability of the IBM SaaS during a Contracted Month

Achieved Service Level (during a Contracted Month)	**Availability Credit (% of Monthly Subscription Fee for Contracted Month which is the subject of a Claim)**
< 99.5%	2%
< 98.0%	5%
< 96.0%	10%

"Achieved Service Level", expressed as a percentage is calculated as: (a) the total number of minutes in a Contracted Month, minus (b) the total number of minutes of Downtime in a Contracted Month, divided by (c) the total number of minutes in a Contracted Month.

Example: 250 minutes total Downtime during Contracted Month

43,200 total minutes in a 30 day Contracted Month - 250 minutes Downtime = 42,950 minutes _____ 43,200 total minutes	= 2% Availability Credit for 99.4% Achieved Service Level during the Contracted Month

3.1 Exclusions

This SLA is made available only to IBM Clients. This SLA does not apply to the following:

- Beta and trial Services.
- Non-production environments, including but not limited to, test, disaster recovery, quality assurance, or development.
- Claims made by an IBM Client's users, guests, participants, and permitted invitees of the IBM SaaS.
- If Client has breached any material obligations under the ToU, including without limitation, breach of any payment obligations.