IBM Trusteer Fraud Protection

This Service Description describes the Cloud Service IBM provides to Client. Client means the contracting party and its authorized users and recipients of the Cloud Service. The applicable Quotation and Proof of Entitlement (PoE) are provided as separate Transaction Documents.

1. Cloud Service

The following Cloud Services are covered by this Service Description:

Rapport Cloud Services:

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport for Retail Premium Support
- IBM Trusteer Rapport II for Business
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications For Retail
- IBM Trusteer Rapport Additional Applications For Business
- IBM Trusteer Rapport Large Redeployment
- IBM Trusteer Rapport Small Redeployment

Pinpoint Cloud Services:

- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Business
- IBM Trusteer Pinpoint Carbon Copy for Business Premium Support

- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Criminal Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

Mobile Cloud Services:

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

- IBM Trusteer Mobile Browser for Retail Premium Support

1.1 Business and Retail Cloud Services

The IBM Trusteer Cloud Services are granted 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. A Retail Application is defined as an online banking application, mobile application or e-commerce application designed to service consumers. Client's policy may classify certain small businesses as eligible for retail access.

b. 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.

1.1.1 Business Cloud Services

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business

1.1.2 Retail Cloud Services

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Retail

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

1.1.3 Additional Cloud Services for IBM Trusteer Rapport

a. Additional Cloud Services available for IBM Trusteer Rapport for Business:
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business
   - IBM Trusteer Rapport Mandatory Service for Business
   - IBM Trusteer Rapport Additional Applications For Business

b. Additional Cloud Services available for IBM Trusteer Rapport for Retail:
   - IBM Trusteer Rapport Fraud Feeds for Retail
   - IBM Trusteer Rapport Phishing Protection for Retail
   - IBM Trusteer Rapport Mandatory Service for Retail
   - IBM Trusteer Rapport Additional Applications For Retail

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

Subscription to IBM Trusteer Rapport for Business or IBM Trusteer Rapport for Retail is a prerequisite to the associated additional Cloud Services listed in this section.

1.1.4 Additional Cloud Services for IBM Trusteer Pinpoint Malware Detection and/or IBM Trusteer Pinpoint Malware Detection II

a. Additional Cloud Services available for IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition or IBM Trusteer Pinpoint Malware Detection for Business Standard Edition or for IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business or IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:
   - IBM Trusteer Pinpoint Carbon Copy for Business
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. Additional Cloud Services available for IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition or IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition or for IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition or IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition:
   - IBM Trusteer Pinpoint Carbon Copy for Retail
   - IBM Trusteer Rapport Remediation for Retail
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

Premium support is available for specific offerings as specified in this document. Subscription to IBM Trusteer Pinpoint Malware Detection for Business or IBM Trusteer Pinpoint Malware Detection for Retail or IBM Trusteer Pinpoint Malware Detection II for Business or IBM Trusteer Pinpoint Malware Detection II for Retail is a prerequisite to the associated additional Cloud Services listed in this section.

1.1.5 Additional Cloud Services for IBM Trusteer Pinpoint Criminal Detection and/or IBM Trusteer Pinpoint Criminal Detection II

a. Additional Cloud Services available for IBM Trusteer Pinpoint Criminal Detection for Business or IBM Trusteer Pinpoint Criminal Detection II:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. Additional Cloud Services available for IBM Trusteer Pinpoint Criminal Detection for Retail and/or IBM Trusteer Pinpoint Criminal Detection II for Retail:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Premium support is available for specific offerings as specified in this document.

Subscription to IBM Trusteer Pinpoint Criminal Detection for Business or IBM Trusteer Pinpoint Criminal Detection for Retail or IBM Trusteer Pinpoint Criminal Detection II for Business or IBM Trusteer Pinpoint Criminal Detection II for Retail is a prerequisite to the associated additional Cloud Services listed in this section.

1.1.6 Additional Cloud Services for IBM Trusteer Pinpoint Detect Standard and/or IBM Trusteer Pinpoint Detect Premium and/or IBM Security Pinpoint Detect Standard with access management integration and/or IBM Security Detect Premium with access management integration

a. Additional Cloud Services available for IBM Trusteer Detect Standard for Business and/or IBM Trusteer Pinpoint Detect Premium for Business and/or IBM Security Pinpoint Detect Standard with access management integration for Business and/or IBM Security Detect Premium with access management integration for Business:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

b. Additional Cloud Services available for IBM Trusteer Detect Standard for Retail and/or IBM Trusteer Pinpoint Detect Premium for Retail and/or IBM Security Pinpoint Detect Standard with access management integration for Retail and/or IBM Security Detect Premium with access management integration for Retail:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Subscription to IBM Trusteer Detect Standard or IBM Trusteer Pinpoint Detect Premium or IBM Security Pinpoint Detect Standard with access management integration or IBM Security Detect Premium with access management integration is a prerequisite to the associated additional Cloud Services listed in this section.

1.1.7 Other Additional Cloud Services

Any additional Cloud Services 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.

1.2 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 Cloud Services coverage.

Account Holder Client Software – means the IBM Trusteer Rapport client-enabling software or the IBM Trusteer Mobile Browser client-enabling software or the any other client-enabling software that is provided with some Cloud Services 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 Trusteer Rapport Cloud Services

2.1 IBM Trusteer Rapport for Retail and/or IBM 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 Trusteer Rapport collects intelligence on active phishing and malware attacks against organizations worldwide. IBM Trusteer Rapport applies behavioral algorithms aimed to block phishing attacks and to prevent the installation and the operation of MitB malware strains.

This Cloud Service 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 Cloud Service offering includes:

a. Trusteer Management Application ("TMA"):

The TMA is made available on the IBM Trusteer cloud-hosted environment, through which the Client (and unlimited number of its authorized personnel) can: (i) view and download certain events data reporting and risk assessments, and (ii) view the configuration of the client-enabling software licensed to the Client's Eligible Participants 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 Cloud Service.

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 Cloud Services 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 Cloud Services 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 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 Trusteer Rapport Mandatory Service Cloud Service 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 IBM Trusteer Rapport II for Retail and/or IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Trusteer Rapport II Cloud Service is a new construction of IBM Trusteer Rapport to help standardize charges related to the protection of multiple Applications and replaces one-off charges when adding Applications.

Trusteer Rapport II 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 Trusteer Rapport collects intelligence on active phishing and malware attacks against organizations worldwide. IBM Trusteer Rapport applies behavioral algorithms aimed to block phishing attacks and to prevent the installation and the operation of MitB malware strains.

This Cloud Service is entitled under the 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 Cloud Service offering includes:

a. Trusteer Management Application ("TMA"):

The TMA is made available on the IBM Trusteer cloud-hosted environment, through which the Client (and unlimited number of its authorized personnel) can: (i) view and download certain events data reporting and risk assessments, and (ii) view the configuration of the client-enabling software licensed to the Client's Eligible Participants 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 Cloud Service.

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 Cloud Services 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 Cloud Services coverage. 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 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 Trusteer Rapport Mandatory Service Cloud Service 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.

Trusteer Rapport II for Business and/or Trusteer Rapport II for Retail each includes protection for one Application. For every additional Application, Client should obtain entitlement to IBM Trusteer Rapport Additional Applications.

2.3 Optional Additional Cloud Services for IBM Trusteer Rapport for Business and/or IBM Trusteer Rapport for Retail and/or IBM Trusteer Rapport II for Business and/or IBM Trusteer Rapport II for Retail

Subscription to IBM Trusteer Rapport Cloud Services or IBM Trusteer Rapport II Cloud Services is a perquisite to subscription to any of the following additional Cloud Services. If the Cloud Service is designated as "for Business", then the additional Cloud Services acquired must also be designated as "for Business". If the Cloud Service is designated as "for Retail", then the additional Cloud Services 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.

2.3.1 IBM Trusteer Rapport Fraud Feeds for Business and/or IBM Trusteer Rapport Fraud Feeds for Retail

When subscribing to this add-on Cloud Service, Client (and unlimited number of its authorized personnel) can use the TMA to view, subscribe, and configure the delivery of threat feeds generated from the Trusteer Rapport Cloud Service. Feeds can be sent by email to designated email addresses or through SFTP as text files.

2.3.2 IBM Trusteer Rapport Phishing Protection for Business and/or IBM 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 Cloud Service 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.

2.3.3 IBM Trusteer Rapport Mandatory Service for Business and/or IBM 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 Cloud Services coverage.

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

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

Client may implement the IBM 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 Cloud Services coverage.

2.3.4 IBM Trusteer Rapport Large Redeployment and/or IBM Trusteer Rapport Small Redeployment

Clients redeploying their online banking Applications during the term of the service and consequently, requiring changes to their deployment of IBM Trusteer Rapport or IBM Trusteer Rapport II should purchase IBM Trusteer Rapport Redeployment Cloud Service.

Redeployment may be due to the Client changing the Application's domain or host URL, applying changes to the splash configuration, or moving to a new on-line banking platform.

For the redeployment transition period of 6 months the Client is entitled to additional Applications on a one to one basis running on top of the already subscribed Applications.

IBM Trusteer Rapport Large Redeployment applies to environments with more than 20,000 users, and IBM Trusteer Rapport Small Redeployment applies to environments with less than or equal to 20,000 users.

2.3.5 IBM Trusteer Rapport Additional Applications for Business and/or IBM Trusteer Rapport Additional Applications for Retail

For IBM Trusteer Rapport II for Business, deployment on any additional Business Application beyond the first Application requires entitlement to IBM Trusteer Rapport Additional Applications for Business Cloud Service. For IBM Trusteer Rapport II for Retail, deployment on any additional Retail Application beyond the first Application requires entitlement to IBM Trusteer Rapport Additional Applications for Retail Cloud Service.

3. IBM Trusteer Pinpoint Cloud Services

IBM 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 Cloud Services coverage and fraud prevention processes.

This Cloud Service includes:

a. TMA:

   The TMA is made available on the IBM Trusteer cloud-hosted environment, through which Client (and unlimited number of its authorized personnel) can: (i) view and download certain event data reporting and risk assessments, and (ii) view, subscribe, and configure the delivery of threat feeds generated from the Pinpoint offerings.

b. Web Script and/or APIs:

   For deployment on a website for the purposes of accessing or using the Cloud Service.

3.1 IBM Trusteer Pinpoint Malware Detection and IBM Trusteer Pinpoint Criminal Detection Best Practices

In the event of malware detection in IBM Trusteer Pinpoint Malware Detection Cloud Services or IBM Trusteer Pinpoint Malware Detection II Cloud Services or account takeover detection in IBM Trusteer Pinpoint Criminal Detection Cloud Services or IBM Trusteer Pinpoint Criminal Detection II Cloud Services, Client must follow the Pinpoint Best Practices Guide. Do not use IBM Trusteer Pinpoint Malware

Detection Cloud Services or IBM Trusteer Pinpoint Malware Detection II Cloud Services or IBM Trusteer Pinpoint Criminal Detection Cloud Services or IBM Trusteer Pinpoint Criminal Detection II Cloud Services 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 Trusteer Pinpoint Cloud Services (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).

3.2 IBM Trusteer Pinpoint Criminal Detection for Business and/or IBM 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 Trusteer Pinpoint Criminal Detection Cloud Services 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 Cloud Services coverage or Client can receive the events data via a backend API delivery mode.

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business and/or IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II is a new construction of IBM Trusteer Pinpoint Criminal Detection to help standardize charges related to the protection of multiple Applications and replaces one-off charges when adding Applications.

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 Trusteer Pinpoint Criminal Detection II Cloud Services 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 Cloud Services coverage or Client can receive the events data via a backend API delivery mode.

   This Cloud Service includes protection of one Application. For every additional Application, Client should obtain entitlement to IBM Trusteer Pinpoint Criminal Detection Additional Applications.

3.4 IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition and/or IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition and/or IBM Trusteer Pinpoint Malware Detection for Business Standard Edition and/or IBM 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 Trusteer Pinpoint Malware Detection Cloud Services 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 Cloud Service as described herein.

3.5 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business and/or IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail and/or IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business and/or IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II is a new construction of IBM Trusteer Pinpoint Malware Detection to help standardize charges related to the protection of multiple Applications and replaces one-off charges when adding Applications.

Clientless detection of Man in the Browser (MitB) financial malware-infected browsers connecting to a Business and/or Retail Application. IBM Trusteer Pinpoint Malware Detection Cloud Services 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 Cloud Service as described herein.

This Cloud Service includes protection of one Application. For every additional Application, Client must obtain entitlement to IBM Trusteer Pinpoint Malware Detection Additional Applications.

3.6 Optional Additional Cloud Services for IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition and/or IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition and/or IBM Trusteer Pinpoint Malware Detection for Business Standard Edition and/or IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition and/or IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail and/or IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business and/or IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail and/or IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- For the IBM Trusteer Rapport Remediation for Retail Cloud Service, there is a prerequisite of IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail or IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail or IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail or IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.

- For the IBM Trusteer Rapport Remediation for Business Cloud Service, there is a prerequisite of IBM Trusteer Pinpoint Malware Detection Standard Edition for Business or IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business or IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business or IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.
- For IBM Trusteer Pinpoint Carbon Copy for Retail, there is a prerequisite of IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail or IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail or IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail or IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- For IBM Trusteer Pinpoint Carbon Copy for Business, there is a prerequisite of IBM Trusteer Pinpoint Malware Detection Standard Edition for Business or IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business or IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business or IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business and/or IBM Trusteer Pinpoint Carbon Copy for Retail

IBM 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 Cloud Service offerings coverage.

3.6.2 IBM Trusteer Rapport Remediation for Retail and/or IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail and IBM Trusteer Rapport Remediation for Business aim 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 Application on an ad-hoc basis, where MitB malware infections have been detected by IBM Trusteer Pinpoint Malware Detection events data. Client must have current subscription to IBM Trusteer Pinpoint Malware Detection or IBM Trusteer Pinpoint Malware Detection II actually running on Client's Application. Client may use this Cloud Service offering only in connection with Eligible Participants who access the Client's Application, and solely as tool that aims to investigate and remediate a particular infected device (PC/MAC) on an ad-hoc basis. The IBM Trusteer Rapport Remediation 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 Application(s) at least once, and Client's configuration must include collection of User IDs. For avoidance of doubt, this Cloud Service 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.

3.6.3 IBM Trusteer Pinpoint Malware Detection Redeployment

Clients redeploying their online banking Applications during the term of the service and consequently, requiring changes to their deployment of IBM Trusteer Pinpoint Malware Detection and/or IBM Trusteer Pinpoint Malware Detection II should purchase IBM Trusteer Pinpoint Malware Detection Redeployment.

Redeployment may be due to the Client changing the Application's domain or host URL, converting the online Application to a new technology, moving to a new on-line banking platform, or adding a new login flow to an existing Application.

For the redeployment transition period of 6 months the Client is entitled to additional Applications on a one to one basis running on top of the already subscribed Applications.

3.6.4 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail and/or IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

For IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business or IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business, deployment on any additional Business Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Malware Detection Additional Applications for Business. For IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail or IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, deployment on any additional Retail Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.

3.7 Optional Additional Cloud Services for IBM Trusteer Pinpoint Criminal Detection for Business and/or IBM Trusteer Pinpoint Criminal Detection for Retail and/or for IBM Trusteer Pinpoint Criminal Detection II for Business and/or IBM Trusteer Pinpoint Criminal Detection II for Retail

3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

Clients redeploying their online banking Applications during the term of the service and consequently, requiring changes to their deployment of IBM Trusteer Pinpoint Criminal Detection Cloud Service should purchase IBM Trusteer Pinpoint Criminal Detection Redeployment.

Redeployment may be due to the Client changing the Application's domain or host URL, converting the online Application to a new technology, moving to a new on-line banking platform, or adding a new login flow to an existing Application.

For the redeployment transition period of 6 months the Client is entitled to additional Applications on a one to one basis running on top of the already subscribed Applications.

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business and/or IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

For IBM Trusteer Pinpoint Criminal Detection II for Business, deployment on any additional Business Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business. For IBM Trusteer Pinpoint Criminal Detection II for Retail, deployment on any additional Retail Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail.

4. IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Suite") is a collection of cloud-based services that is designed to provide a layer of fraud protection and can integrate with additional IBM products to provide a life cycle management solution. The Suite includes the following cloud-based services:

- IBM Trusteer Pinpoint Detect that aims to detect and mitigate malware, phishing and account takeover attacks. Trusteer Pinpoint Detect can be integrated into Client's Business and/or Retail Applications for which Client has subscribed to Cloud Service coverage and fraud prevention processes.
- IBM Trusteer Rapport for Mitigation that aims to remediate and protect infected end-points.

The Cloud Services include:

a. TMA:

   The TMA is made available on the IBM 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. 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 Cloud Service coverage or Client can receive the events data via a backend API delivery mode.

c. Web Script and/or APIs:

   For deployment on a website for the purposes of accessing or using the Cloud Service.

Pinpoint Best Practices

In the event of malware detection or account takeover detection, Client must follow the Pinpoint Best Practices Guide. Do not use IBM Trusteer Pinpoint Detect Cloud Services 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 Trusteer Pinpoint Detect 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).

4.1 IBM Trusteer Pinpoint Detect Standard for Business and/or IBM Trusteer Pinpoint Detect Standard for Retail

This Cloud Service combines the Cloud Services IBM Trusteer Pinpoint Criminal Detection and IBM Trusteer Pinpoint Malware Detection to offer a single, unified solution.

The solution helps with clientless detection of malware and/or 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 Trusteer Pinpoint 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.

Standard support (as defined in the Technical Support section below) is included in this Cloud Service. For Premium support, Client must purchase Detect Premium.

This Cloud Service includes protection of one Application. For every additional Application, Client should obtain entitlement to IBM Trusteer Pinpoint Detect Standard Additional Applications.

4.2 IBM Trusteer Pinpoint Detect Premium for Business and/or IBM Trusteer Pinpoint Detect Premium for Retail

This Cloud Service combines IBM Trusteer Pinpoint Criminal Detection and IBM Trusteer Pinpoint Malware Detection to offer a single, easy to integrate unified solution.

The solution helps with clientless detection of malware and/or 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 Trusteer Pinpoint 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.

The service includes enhanced functionality and services, including: extended deployment and set up services, tailored security policies, investigation services, etc.

This Cloud Service includes protection of one Application. For every additional Application, Client should obtain entitlement to IBM Trusteer Pinpoint Detect Premium Additional Applications.

Premium support is included in this Cloud Service.

Pinpoint Detect Policy Manager:

The Policy Manager is included in Pinpoint Detect Premium service and is made available on the IBM Trusteer cloud-hosted environment, through which Client (and unlimited number of authorized personnel) can: (i) design, test and deploy to production environment logic to detect fraudulent activity, (ii) design reports and dashboards, and (iii) view, configure, and set security policies and policies to detect suspicious activity on customer Application.

Consultancy services are required for activation of the Policy Manager feature and for extra deep dive required support. Consultancy services details will be outlined separately in a statement of work.

When Policy Manager is activated, IBM reserves the right to access the Client's environment for support purposes to adjust Client's policies to remediate major issues that are derived from policy changes.

Client commits to protect any data that is exposed through the Policy Manager from misuse.

When the Policy Manager feature is activated, the Client must follow IBM guidelines for rules setting, as outlined in the documentation. Client acknowledges that IBM is not liable for any situation that may derive from the Client not following those recommendations.

Any stability and/or service degradation issues that may arise due to mis-configuration of the Policy Manager feature by the Client will not be considered as Downtime for the SLA calculation.

4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business and/or IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

IBM Trusteer Pinpoint Detect Standard with access management integration Cloud Service includes the functionality of IBM Security Pinpoint Detect Standard as detailed in section 4.1 above.

IBM Trusteer Pinpoint Detect Standard with access management integration is used when purchased with access management systems, such as IBM Security Access Management ("ISAM"). When purchased with ISAM both offerings must be enabled. This offering includes the integration option with the access management system. It does not include the entitlement for the access management system.

This offering includes protection of one Application. For every additional Application, Client should obtain entitlement to IBM Trusteer Pinpoint Detect Standard Additional Applications.

Standard support (as defined in the Technical Support section) is included in this Cloud Service. IBM Trusteer Pinpoint Detect Premium with access management integration for Business and/or IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

IBM Trusteer Pinpoint Detect Premium with access management integration Cloud Service includes the functionality of IBM Security Pinpoint Detect Premium as detailed in section 4.2 above, and the integration option with the access management system.

IBM Trusteer Pinpoint Detect Premium with access management integration is used when purchased with access management systems, such as IBM Security Access Management ("ISAM"). When purchased with ISAM both offerings must be enabled. This Cloud Service includes the integration option with the access management system. It does not include the entitlement for the access management system.

This Cloud Service includes protection of one Application. For every additional Application Client should obtain entitlement to IBM Trusteer Pinpoint Detect Premium Additional Applications.

Premium support is included in this offering.

4.4 Optional services for IBM Trusteer Pinpoint Detect Standard and/or IBM Trusteer Pinpoint Detect Premium

For the Cloud Services in this section, there is a prerequisite of entitlement to IBM Trusteer Pinpoint Detect Premium for Retail or IBM Trusteer Pinpoint Detect Standard for Retail.

4.5 IBM Trusteer Rapport for Mitigation for Retail and/or IBM Trusteer Rapport for Mitigation for Business

IBM Trusteer Rapport for Mitigation aims to investigate, remediate, block and remove 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 malware infections have been detected by IBM Trusteer Pinpoint Detect Premium or IBM Trusteer Pinpoint Detect Standard events data. Client must have a current subscription to IBM Trusteer Pinpoint Detect Premium or IBM Trusteer Pinpoint Detect Standard actually running on Client's Retail Application. Client may use this Cloud Service 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 Trusteer Rapport for Mitigation 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 Cloud Service 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.

4.5.1 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business and/or IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail and/or IBM Trusteer Pinpoint Detect Premium Additional Applications for Business and/or IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

For IBM Trusteer Pinpoint Detect Standard for Business deployment on any additional Business Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

For IBM Trusteer Pinpoint Detect Standard for Retail deployment on any additional Retail Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.

For IBM Trusteer Pinpoint Premium for Business deployment on any additional Business Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

For IBM Trusteer Pinpoint Premium for Retail deployment on any additional Retail Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.

4.5.2 IBM Trusteer Pinpoint Detect Standard Redeployment and/or IBM Trusteer Pinpoint Detect Premium Redeployment

Clients redeploying their online banking Applications during the term of the service and consequently, requiring changes to their deployment of IBM Trusteer Pinpoint Detect should purchase IBM Trusteer Pinpoint Detect Redeployment.

Redeployment may be due to the client changing the Application's domain or host URL, converting the online Application to a new technology, moving to a new on-line banking platform, or adding a new login flow to an existing Application.

For the redeployment transition period of 6 months the Client is entitled to additional Applications on a one to one basis running on top of the already subscribed Applications.

5. IBM Trusteer Mobile Cloud Services

5.1 IBM Trusteer Mobile Browser for Business and/or IBM Trusteer Mobile Browser for Retail

IBM 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 Cloud Services coverage, mobile devices' risk assessment, and phishing protection. Secure Wi-Fi detection is only available for Android platforms. For the purpose of this Cloud Service mobile devices include mobile phones or tablets and do not include Laptop PCs and Macs.

Through the TMA, Client 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 Cloud Services 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 Cloud Services 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 Cloud Services 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 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.

5.2 IBM Trusteer Mobile SDK for Business and/or IBM Trusteer Mobile SDK for Retail

IBM Trusteer Mobile SDK Cloud Services 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 Cloud Services coverage, devices' risk assessment, and pharming protection. Secure Wi-Fi detection is only available for Android platforms.

IBM Trusteer Mobile SDK Cloud Services 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 Trusteer mobile library as well as the "Run-time Component", or "Redistributable", a proprietary code generated by the IBM 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 Cloud Services coverage. ("Client Integrated Mobile App").

IBM Trusteer Mobile SDK for Retail is available in packs of 100 Eligible Participants or packs of 100 Client Devices, and IBM 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 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 Service Description; 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 solely responsible for development, testing and support of Client Integrated Mobile App. 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 Cloud Services.

IBM has tested sample applications created with the mobile tools provided in the IBM 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.

Source Components and Sample Materials – The IBM Trusteer Mobile SDK may include some components in source code form ("Source Components") and other materials identified as Sample Materials. Client may copy and modify Source Components and Sample Materials for internal use only provided such use is within the limits of the license rights under this Agreement, provided however that

Client may not alter or delete any copyright information or notices contained in the Source Components or Sample Materials. IBM provides the Source Components and Sample Materials without obligation of support and "AS IS", WITH NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTY OF TITLE, NON-INFRINGEMENT OR NON-INTERFERENCE AND THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Note that the Source Components or Sample Materials are provided solely as an example of how to implement the Embeddable into the CIMA, the Source Components or Sample Materials may not be compatible with Client's development environment, and Client is solely responsible for the testing and the implementation of the Embeddable into its CIMA.

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 Trusteer Mobile SDK is in compliance with terms of this Service Description.

6. Premium Support

Client is entitled to Premium Support only for Cloud Services for which Client has subscribed to the associated Premium Support offering.

7. Deployment of IBM Trusteer Fraud Protection

For each Application to which Client subscribes, Client's base subscription includes required setup and initial deployment activities on IBM Trusteer cloud, including initial one-time startup, configuration, Splash Template, testing and training.

Deployment activities do not include the implementation activities that are required on Client's Applications or systems.

The implementation phase of the various Cloud Services is designed to be implemented in the time frames as detailed in the relevant deployment guides.

The completion of these implementation phases within the allotted time frame depends upon the full commitment and participation of Client's management and personnel. Client should provide the required information in a timely fashion. IBM's performance is predicated upon Client's timely information and decisions and any delay may result in additional costs and/or delay of the completion of these implementation services.

For each Application for which Client subscribes for, client's base subscription includes required setup and initial deployment activities on IBM Trusteer cloud, including initial one-time startup, configuration, Splash Template, testing and training.

Client's subscription includes support and testing for the pages within such Client's application that will be tagged as recommended by IBM in the initial deployment. IBM is not responsible for: (i) partial deployment, (ii) Client's election not to deploy the IBM cloud services as recommended by IBM, or (iii) Client's election to conduct the deployment, setup and testing on its own. (IV) Partial deployment or protection result from inadequate information provided by the Client. Additional services, including deployment activities beyond the initial deployment, may be contracted for an additional charge under a separate agreement.

8. Data Privacy and Security

This Cloud Service follows IBM's data security and privacy principles for Cloud Services which are available at http://www.ibm.com/cloud/data-security and any additional terms provided in this section. Any change to IBM's data security and privacy principals will not degrade the security of the Cloud Service.

This Cloud Service may be used to process content that contains personal data if Client, as the data controller, determines that the technical and organizational security measures are appropriate to the risks presented by the processing and the nature of the data to be protected. Client recognizes that this Cloud Service does not offer features for the protection of sensitive personal data or data subject to additional regulatory requirements.

This Cloud Service is included in IBM's Privacy Shield certification and applies when Client chooses to have the Cloud Service hosted in a data center located in the United States, and is subject to IBM's Privacy Shield Privacy Policy, available at http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Security Features and Responsibilities

The Cloud Service implements the following security features:

The Cloud Service encrypts content during data transmission to and from the IBM network and when awaiting data transmission from the endpoint.

8.2 Lawful Use and Consent

Lawful Use

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

Authorization to Collect and Process Data

The Cloud Service will collect information from Eligible Participants and Client Devices who interact with the Business or Retail Applications for which Client has subscribed to Cloud Service coverage. The Cloud Service 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 Cloud Service. 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 Service Description.

For IBM Trusteer offerings that include the Trusteer Management Application (TMA):

The following data is collected and stored in the Trusteer Management Application (TMA) for TMA administrators from the sponsoring enterprise: email address (as login), hashed password, given name, surname, job title, and department.

For IBM Trusteer Pinpoint Cloud Services:

Collected data may include:

- user or endpoint identifiers such as encrypted or one-way hashed User ID, Persistent User ID (PUID), Rapport Agent Key, and the Customer Session ID;
- data related to the protected application, such as specific attributes/elements from the customers' online banking application as rendered in the end user's browser, website visits and browsing history;
- installed software environment information, browser and device attributes and settings, and browser history length;
- hardware information and timestamp;
- browser headers and communication protocol data, such as user IP address, cookies, referrer header, and other HTTP headers;
- end user mouse movement data, such as the mouse pointer coordinates, clicks, and scroll wheel movement (and their equivalents) and timestamp while interacting with Client's online banking application;
- phishing sites and information submitted into phishing sites; and
- at Client's sole option, transactional data (transaction amount, transaction currency and destination codes, one-way hashed transaction target bank identifier, one-way hashed transaction target account identifier, binary value if transaction is a new payee, and transaction date/time) and optional risk data score.
- at Client's sole option, typing rhythms on the keyboard and keystroke family sequences used by the end user to enter a username, password, and other text (but not the letters, numbers, or special characters themselves, and without ability to discern the username or password);

When Policy Manager is activated, all extended data that is used is Client's sole responsibility. IBM recommends to hash or encrypt any data that may be considered as Personal Identifiers.

Client understands and agrees that IBM is not collecting, storing, managing or maintaining the official books and/or records of Client.

When Client subscribes to IBM Trusteer Rapport for Remediation offering, or in some Pinpoint support cases, IBM may recommend that Rapport's Account Holder Client Software be installed on an Eligible Participant's machine in order to research and investigate suspected malware infection. Collected data for Rapport offerings are set forth below.

For IBM Trusteer Rapport Cloud Services (including Rapport for Remediation or Rapport for Mitigation when deployed in connection with the Pinpoint offerings):

Collected data may include:

- URLs and Internet protocol (IP) addresses of websites that an Account Holder visits that IBM deems to be potentially fraudulent, phishing or exploitive, together with information on the nature of the identified threats;
- URLs and IP addresses of websites Account Holder visits that are controlled by Client and protected by the Cloud Service, such as online banking sites; Account Holder's IP addresses;
- information about the hardware identification, operating systems, application software, peripheral hardware, security configuration, system settings, and network connections of the end point, as well as the ID, name, use patterns, and other identifiable information of the end point;
- information related to program's installation and operation, the program's ID, program's version, security events generated from end point, and information about the program's errors;
- usage statistics and statistical information about threats detected by the program; log files containing browser crashes, infection date and time, and information about the nature of the identified threats or malfunction;
- Client affiliation, also referenced as a Sponsoring Enterprise. An affiliation is established when an end user downloads Rapport from Client's website, selects a particular Client when downloading Rapport from the Trusteer support site, or logs on to Client's banking application. An end user may have more than one Client affiliation;
- a copy of the encrypted User ID that Account Holder uses to interact with Client (optional);
- an encrypted copy of a credit card number that Account Holder enters into a site after the program informs Account Holder that the program deems the site risky;
- files and other information from the end point that IBM security experts suspect may be related to malware or other malicious activity, or that may be associated with general program malfunction; and
- Personal contact information, including name and email, when the end user contacts Support.

For IBM Trusteer Mobile SDK offerings and IBM Trusteer Mobile Browser Cloud Services:

Collected data may include:

- user identifiers, such as encrypted or one-way hashed User ID;
- device information, such as IP address, hashed device ID, timestamp, installed package MD5 values and other device hardware and software information;
- Mobile SDK or Mobile Browser version and date of installation;
- visits to protected applications;
- Client affiliation; and
- device risk data (e.g., presence of malware, root hiders, Wi-Fi encryption status, whether a device is jailbroken);
- crash stack trace (in the event of an unexpected application termination);
- phone build data (e.g., model, manufacturer);
- end users touch screen interactions including x, y coordinates, touch area, and action type (down, up and move);
- motion sensor data, power/resources usage, connectivity settings, environment sensors such as temperature, light and air pressure as well as general device settings (volume, ringer, screen brightness etc.).

8.3 Informed Consent from Data Subjects

For IBM Trusteer Pinpoint Cloud Services and for IBM Trusteer Mobile SDK Cloud Services:

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

For IBM Trusteer Rapport Cloud Services (including Rapport Remediation or Rapport for Mitigation when deployed in connection with the Pinpoint Cloud Services), and IBM Trusteer Mobile Browser Cloud Services:

Client authorizes IBM to obtain fully informed consents necessary to enable lawful use of the Cloud Service 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 Cloud Service and to permit collection and processing of the information by IBM as Client's data processor through the Cloud Service.

8.4 Use of Security Data

As part of the Cloud Service, that include reporting activities, IBM will prepare and maintain de-identified and/or aggregate information collected from the Cloud Service ("Security Data"). The Security Data will not identify the Client, its Eligible Participants, or an individual except as provided in (d) below. Client agrees that IBM may perpetually use and/or copy the Security Data only for the following purposes:

a. publishing and/or distributing the Security Data (e.g., in compilations and/or analyses related to cybersecurity);

b. developing or enhancing products or services;

c. conducting research internally or with third parties;

d. lawful sharing of confirmed third party perpetrator information; and

e. de-identified rules from the Policy Manager.

8.5 Cross Border Transfers

Client agrees that IBM may process the content, including any Personal Data as identified in the section titled Lawful Use and Consent above, 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.

8.6 Data Privacy

If Client makes Personal Data available to the Cloud Service 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 Cloud Service offering available in accordance with IBM's published descriptions of Cloud Services and Client agrees that any such processing is in accordance with Client's instructions. IBM will provide reasonable advance notice via the Customer Portal if IBM makes a material change to the processing location or the way it secures Personal Data as part of the Cloud Service. Client may terminate the current subscription period for the affected Cloud Service, by providing written notice to IBM within thirty (30) days of IBM's notification of the change to Client.

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.

a. Client agrees that for services 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	Germany
IBM Ireland Ltd.	Processor	Ireland
IBM Israel Ltd.	Processor	Israel

For services provided through the Germany data center, some customer support services may be provided by Trusteer employees based in any European Union country.

b. Client agrees that for services 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	Japan, as stated on the Transaction Document
Amazon Web Services (Japan)	Sub-processor	Japan
IBM Ireland Ltd.	Processor	Ireland
IBM Israel Ltd.	Processor	Israel

c. Client agrees that for services provided via the US data center, 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	United States
IBM Ireland Ltd.	Processor	Ireland
IBM Israel Ltd.	Processor	Israel
IBM Corp	Processor	United States

d. For services provided through the data centers listed in Section 8.5.c above, "US data center", IBM may also process through one or more of the following applicable sub-processors, as determined during the provisioning process:

Name of Processor/Sub-processor	Role (Data Processor or Sub-processor)	Location
Amazon Web Services (Australia)	Sub-processor	Australia
Amazon Web Services (Singapore)	Sub-processor	Singapore
Amazon Web Services (Ireland)	Sub-processor	Ireland

e. Client agrees that IBM may, on notice via the Customer Portal, migrate the processing from Amazon Web Services onto IBM's data centers. In addition, IBM may, on notice via the Customer Portal, vary the lists of sub-processors above.

f. The Account Holder's data will be processed in the region from where the Account Holder originally installed the Account Holder Client Software. This may mean that the Account Holder's content may be processed in both the originating region as well as the region agreed to with the Client.

g. Customer support data is stored on a Salesforce.com cloud server that is located in Ireland.

h. For purposes of clarification, because Trusteer Fraud Protection is an integrated solution, if Client terminates one of these Cloud Services, IBM may retain Client data for purposes of providing remaining Cloud Services to Client pursuant to this Service Description.

9. Service Level Agreement

IBM provides the following availability service level agreement ("SLA") for the Cloud Service as specified in a PoE. The SLA is not a warranty. The SLA is available only to Client and applies only to use in production environments.

9.1 Availability Credits

Client must log a Severity 1 support ticket with the IBM technical support help desk within 24 hours of first becoming aware of an event that has impacted the Cloud Service availability. Client must reasonably assist IBM with any problem diagnosis and resolution.

A support ticket claim for failure to meet an SLA must be submitted within three business days after the end of the contracted month. Compensation for a valid SLA claim will be a credit against a future invoice for the Cloud Service based on the duration of time during which production system processing for the Cloud Service is not available ("Downtime"). Downtime is measured from the time Client reports the event until the time the Cloud Service is restored and does not include time related to a scheduled or announced maintenance outage; causes beyond IBM's control; problems with Client or third party content or technology, designs or instructions; unsupported system configurations and platforms or other Client errors; or Client-caused security incident or Client security testing. IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service during each contracted month, as shown in the table below. The total compensation with respect to any contracted month cannot exceed 10 percent of one twelfth (1/12th) of the annual charge for the Cloud Service.

9.2 Service Levels

Availability of the Cloud Service during a contracted month

Availability during a contracted month	Compensation (% of monthly subscription fee* for contracted month that is the subject of a claim)
< 99.5%	2%
< 98.0%	5%
< 96.0%	10%

* If the Cloud Service was acquired from an IBM Business Partner, the monthly subscription fee will be calculated on the then-current list price for the Cloud Service in effect for the contracted month which is the subject of a claim, discounted at a rate of 50%. IBM will make a rebate directly available to Client.

Service Levels and associated Service Credits are measured separately per Cloud Service and per Client Application.

When calculating SLA credits for Cloud Services based on Application entitlements, Availability will be calculated based on the following guidelines:

- Each Application will have an assigned weighted share based on the counted number of sessions' volume during the contracted month.
- Downtime of each Cloud Service per Application will be accumulated separately for the contracted month.

The following is an example of a calculation for one month of activity and associated weighting. This is for illustration purposes only:

Retail Applications	Share out of the total # of sessions in a given contracted month	Total Downtime During contracted month	Weighted Minutes of Downtime
Retail Application A	40%	300 minutes	40% x. 300 minutes = 120 minutes
Retail Application B	20%	250 minutes	20% x 250 minutes = 50 minutes
Retail Application C	40%	150 minutes	40% x 150 minutes = 60
			Total weighted minutes Downtime = 230

Availability, expressed as a percentage, is calculated as: the total number of minutes in a contracted month, minus the total number of weighted minutes of Downtime in the contracted month, divided by the total number of minutes in the contracted month. Sample calculation based on the above weighting example is as follows:

43,200 total minutes in a 30 day contracted month - 230 minutes weighted Downtime = 42,970 minutes _____ 43,200 total minutes	= 2% Availability credit for 99.4% availability during the contracted month

10. Technical Support

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

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 Cloud Service, a Premium Support subscription is available for an additional charge, with the exception of IBM Trusteer Mobile SDK Cloud Services and IBM Trusteer Rapport Mandatory Service Cloud Services. Please contact your IBM Sales representative or IBM Business Partner.

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 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 and callback request.
- 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 Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

11. Entitlement and Billing Information

11.1 Charge Metrics

The Cloud Service is available under the charge metric specified in the Transaction Document:

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

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

   For entitlement purposes of these Cloud Services, an Eligible Participant is an end user of a Client, who has unique login credentials to a Business or Retail Application of the Client.

b. Client Device is a unit of measure by which the Cloud Service 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 Cloud Service during the measurement period specified in Client's Transaction Document.

c. Application is a unit of measure by which the Cloud Service can be obtained. An Application is a uniquely named software program. Sufficient entitlements must be obtained for each Application made available to access and use during the measurement period specified in Client's PoE or Transaction Document.

   For the Cloud Service, an application is a single Business or Retail Application of the Client.

d. Engagement is a unit of measure by which the services can be obtained. An Engagement consists of professional and/or training services related to the Cloud Services. Sufficient entitlements must be obtained to cover each Engagement.

12. Compliance and Auditing

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

An audit may be conducted by IBM to verify compliance with maximum quantity of Applications, Eligible Participants and/or Client Devices.

13. Term and Renewal Options

The term of the Cloud Service begins on the date IBM notifies Client of their access to the Cloud Service, as documented in the PoE. The PoE will specify whether the Cloud Service renews automatically, proceeds on a continuous use basis, or terminates at the end of the term.

For automatic renewal, unless Client provides written notice not to renew at least 90 days prior to the term expiration date, the Cloud Service will automatically renew for the term specified in the PoE.

For continuous use, the Cloud Service will continue to be available on a month to month basis until Client provides 90 days written notice of termination. The Cloud Service will remain available to the end of the calendar month after such 90 day period.

14. Additional Terms

14.1 Enabling Software

This Cloud Service includes enabling software, which may be used only in connection with Client's use of the Cloud Service and only for the Cloud Service term.

14.2 IBM Trusteer Annual Subscription Fee Increase

IBM reserves the right to adjust the subscription fee for the Cloud Services. The subscription fee adjustment will be reflected in the prices specified in and for the term of the applicable Quotation. Additional subscription fee adjustments which will be applicable no more than once every twelve (12) months by a percentage to be determined by IBM not to exceed 3% may apply when the term of the Cloud Services is extended through auto renewal or continuous use. These fee adjustments do not alter Client's entitlement to the Cloud Services or the charge metric by which the Cloud Service is obtained. IBM Business Partners are independent from IBM and unilaterally determine their prices and terms.