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:

Pinpoint Assure Cloud Services:

- IBM Trusteer Pinpoint Assure
- IBM Trusteer Pinpoint Assure Application
- IBM Trusteer Mobile Carrier Intelligence

Rapport Cloud Services:

- IBM Trusteer Rapport for Business Premium Support
- 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 Standard Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail

- IBM Trusteer Pinpoint Malware Detection Advanced Edition II 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 Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- 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 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 Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail Premium Support
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Project Management and Consultancy Services
- IBM Trusteer Security Research Consultancy Services
- IBM Trusteer Training Services
- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application
- IBM Trusteer Pinpoint Detect Standard
- IBM Trusteer Pinpoint Detect Premium
- IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect
- IBM Trusteer Pinpoint Verify

Mobile Cloud Services:

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail

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 II for Business
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer Mobile SDK for Business

1.1.2 Retail Cloud Services

- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Mobile SDK 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 II

a. Additional Cloud Services available for IBM Trusteer Rapport II 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 II 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 II for Business or IBM Trusteer Rapport II 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 II

a. Additional Cloud Services available for IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business or IBM Trusteer Pinpoint Malware Detection Standard Edition II 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 Advanced Edition II for Retail or IBM Trusteer Pinpoint Malware Detection Standard Edition II 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 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 Detect Standard and/or IBM Trusteer Pinpoint Detect Premium and/or IBM Trusteer Pinpoint Detect Standard for Retail and/or IBM Trusteer Pinpoint Detect Premium for Retail and/or IBM Trusteer Pinpoint Detect Standard for Business and/or IBM Trusteer Pinpoint Detect Premium for Business

a. Additional Cloud Services available for IBM Trusteer Detect Standard for Business and/or 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 Digital Content Pack for Business
   - IBM Trusteer New Account Fraud for Business

b. Additional Cloud Services available for IBM Trusteer Detect Standard for Retail and/or IBM Trusteer Pinpoint Detect Premium for Retail:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
   - IBM Trusteer Digital Content Pack for Retail
   - IBM Trusteer New Account Fraud for Retail

c. Additional Cloud Services available for IBM Trusteer Pinpoint Detect Standard and/or IBM Trusteer Pinpoint Premium:
   - IBM Trusteer Pinpoint Detect Standard Application
   - IBM Trusteer Pinpoint Detect Premium Application

d. Additional Cloud Services available for IBM Trusteer Pinpoint Detect Premium
   - IBM Trusteer Pinpoint Verify

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

1.1.6 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 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.

1.3 IBM Trusteer Rapport Cloud Services

1.3.1 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 or the Client Device charge metric. The Business offering is sold in packs of 10 Eligible Participants or 10 Client Devices. The Retail offering is sold in packs of 100 Eligible Participants or 100 Client Devices.

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.

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

Subscription to IBM Trusteer Rapport II Cloud Services is a prerequisite 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 or Client Devices 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.

1.3.3 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.

This offering is applicable only under the Eligible Participant charge metric.

1.3.4 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.

This Cloud Service is entitled under the Eligible Participant charge metric or the Client Device charge metric. The Business offering is sold in packs of 10 Eligible Participants or 10 Client Devices. The Retail offering is sold in packs of 100 Eligible Participants or 100 Client Devices.

Premium support can be obtained for this cloud services, under the Eligible Participant charge metric or the Client Device charge metric. The Business offering is sold in packs of 10 Eligible Participants or 10 Client Devices. The Retail offering is sold in packs of 100 Eligible Participants or 100 Client Devices.

1.3.5 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.

This Cloud Service is entitled under the Eligible Participant charge metric. The Business offering is sold in packs of 10. The Retail offering is sold in packs of 100 Eligible Participants.

1.3.6 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 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.

1.3.7 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.

1.4 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.

1.4.1 IBM Trusteer Pinpoint Malware Detection

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

1.4.2 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 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, with 1000 packs of 100 Eligible Participants for Retail, or 1000 packs of 10 Eligible Participants for Business.

c. Standard Edition:

The Standard Editions for Business and/or Retail are fast-to-deploy solutions 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.

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

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

IBM Trusteer Rapport Remediation 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 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.

1.4.5 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 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.

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

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

1.5 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 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).

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

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 Retail or Business 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 Retail or Business 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 Pinpoint Standard Premium Support.

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

The service is available to be purchased by packs of 100 Eligible Participants or by packs of 100 Connections. In case the Client chooses to purchase the service by Connections, Additional Application charge is applicable from the first application.

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

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 Retail or Business 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. The service includes up to 200 hours of shared resource for deployment services per application, and 200 hours of shared resource for security analysis per application upon set-up. The on-going services includes 20 hours of deployment maintenance per year per application, and 100 hours of security research per application per year. Any additional effort is subject to an additional charge.

Pinpoint Detect can consume transactions from both Mobile and Web channels. In case Mobile transactions are included the Pinpoint by Connection is applicable. 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.

The IBM Trusteer Pinpoint Detect Premium for Retail and Business services are available to be purchased by packs of 100 Eligible Participants or IBM Trusteer Pinpoint Detect Premium by packs of 100 Connections. In case the Client chooses to purchase the service by Connections, Additional Application charge is applicable from the first application.

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.

1.5.3 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 or IBM Trusteer Pinpoint Detect Standard.

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

- IBM Trusteer Rapport for Mitigation for Retail 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.
- IBM Trusteer Rapport for Mitigation for Business aims to investigate, remediate, block and remove malware infections from infected devices (PC/MACs) of Client's Eligible Participants who access the Client's Business 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 Business Application. Client may use this Cloud Service only in connection with Eligible Participants who access the Client's Business 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 Business 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 Business 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.

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

The service includes up to 200 hours of shared resource for deployment services per application, and 200 hours of shared resource for security analysis per application upon setup. The on-going services include 20 hours of deployment maintenance per year per application, and 100 hours of security research per application per year.

- For an IBM Trusteer Pinpoint Detect Standard for Retail deployment of any additional Retail Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.
- For an IBM Trusteer Pinpoint Detect Standard for Business deployment of any additional Business Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.
- For an IBM Trusteer Pinpoint Premium for Retail deployment of any additional Retail Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.
- For an IBM Trusteer Pinpoint Premium for Business deployment of any additional Business Application beyond the first Application requires entitlement to IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

1.5.6 IBM Trusteer Pinpoint Detect Standard Application and/or IBM Trusteer Pinpoint Detect Premium Application

This service is applicable for Web and Mobile channels.

The service includes up to 200 hours of shared resource for deployment services per application, and 200 hours of shared resource for security analysis per application upon setup. The on-going services include

20 hours of deployment maintenance per year per application, and 100 hours of security research per application per year

- IBM Trusteer Pinpoint Detect Standard deployment requires entitlement to IBM Trusteer Pinpoint Detect Standard Application for every Application.
- IBM Trusteer Pinpoint Premium deployment requires entitlement to IBM Trusteer Pinpoint Detect Premium Application for every Application.

1.5.7 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.

1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support and/or IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Clients that purchase the Pinpoint Detect Standard Cloud Service can purchase Premium Support service. The scope of the Premium Support services is listed in section 4 below.

1.5.9 IBM Trusteer Digital Content Pack for Retail and/or IBM Trusteer Digital Content Pack for Business

The IBM Trusteer Digital Content Pack enables security analysts to integrate new fraud models while fully supporting the creation and modification of ad-hoc models to react to evolving threats. It consists of an extensive set of rules, insights, and policies that can be purchased as an additional and integral part of the solution. The Digital Content Pack helps to further tighten the integration between Trusteer's digital fraud prevention capabilities and the IBM Safer Payments cashless-payments channels. By leveraging its built-in rules and specific business-logic, the Digital Content Pack enables banks and other financial institutions to further enhance existing fraud detection and prevention capabilities.

The IBM Trusteer Digital Content Pack for Retail is available in packs of 100 Eligible Participants. The IBM Trusteer Digital Content Pack for Business is available in packs of 10 Eligible Participants.

Consultancy services are required for the integration of the Digital Content Pack with Pinpoint Detect and IBM Safer Payments, as well as for support services requiring significant attention. Consultancy services are acquired separately pursuant to a separate statement of work.

1.5.10 IBM Trusteer New Account Fraud for Retail and/or IBM Trusteer New Account Fraud for Business

This service, available to Pinpoint subscribers is designed to detect anomalies, flag suspicious activities, and generate alerts early in the new account creation process. The service monitors new accounts to identify new activity associated with fraud post-account and young account profiling to provide an early warning sign that the new account may be a mule account or used to conduct fraud, through usage reports available in the TMA.

The IBM Trusteer New Account Fraud for Retail and the IBM Trusteer New Account Fraud for Business are available in packs of 10 API Calls.

1.5.11 IBM Trusteer Pinpoint Verify

Client must have a current subscription to IBM Trusteer Pinpoint Detect Premium prior to subscribing to this Cloud Service.

This Cloud Service provides capabilities to challenge users for a second factor of authentication in order to verify their identities when accessing a digital service. It is available for Pinpoint Detect Premium, in order to provide a second authentication factor for protected applications. The decision on when to challenge users for second factor authentication is derived by the protected application, and can be based on the recommendations returned by the Pinpoint Detect Premium platform or any other policies defined by the protected application.

1.6 IBM Trusteer Pinpoint Assure

This service flags suspicious activities and generate alerts in the new account creation / registration process. The service monitors the account registration process to identify activity associated with fraud to provide an early warning sign that the new account may be a mule account or used to conduct fraud, through usage reports available in the TMA.

The IBM Trusteer Pinpoint Assure is available in packs of 100 Connections.

1.6.1 Optional services for IBM Trusteer Pinpoint Assure

1.6.2 IBM Trusteer Pinpoint Assure Application

For IBM Trusteer Pinpoint Assure deployment on any Application requires entitlement to IBM Trusteer Pinpoint Assure Application.

The IBM Trusteer Pinpoint Assure is available to be purchased by application.

1.6.3 IBM Trusteer Mobile Carrier Intelligence and/or IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Client must have a current subscription to either IBM Trusteer Pinpoint Assure or IBM Trusteer Pinpoint Detect prior to subscribing to this Cloud Service.

This Cloud Service enhances IBM Trusteer Pinpoint Assure and/or IBM Trusteer Pinpoint Detect by providing additional information and context around mobile numbers provided to either of those Cloud Services, helping to determine the fraud risk of a given session. Client may query the Cloud Service to learn characteristics about a given mobile number, such as the carrier information associated with that number.

Data provided by this Cloud Service regarding mobile numbers ("Mobile Intelligence") may be used only for Client's internal purposes, and may only be retained for a period of thirty (30) days. Client must requery the Cloud Service regarding the same mobile number after such period to obtain Mobile Intelligence regarding that number and may not simply re-use Mobile Intelligence received from a previous query. Client may not cache, except as permitted above, re-use, or use in conjunction in-whole or in-part with any data mining or to archive any of the Mobile Intelligence.

1.7 IBM Trusteer Remotely Delivered Services

IBM Trusteer Remotely Delivered Services are available as an optional add-on for Pinpoint Detect Premium and Pinpoint Assure Cloud Services.

1.7.1 IBM Trusteer Project Management and Consultancy Services

This service provides up to 200 hours of consultancy services during which IBM will perform some or all of the following:

a. Initial set up services: frequent periodical meetings, project management services

b. Policy Manager: on-going support

The offering is available to be purchased by Engagement.

1.7.2 IBM Trusteer Security Research Consultancy Services

This consultancy service includes up to 200 hours of shared resource for security analysis to provide additional services on top of the defined solution and premium support (when applicable), and includes:

a. Extended fraud research: weekly meetings and training.

b. High priority Client's release support

c. On-going customized rules investigation and support

The offering is available to be purchased by Engagement.

1.7.3 IBM Trusteer Training Services

This consultancy service is designed to provide additional services on top of the defined solution and premium support (when applicable), and includes training services on Trusteer portfolio for Client's employees.

The offering is available to be purchased by Engagement.

1.8 IBM Trusteer Mobile Cloud Services

1.8.1 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 does not guarantee that any application or output creating using mobile tools included with the IBM Security Mobile SDK will function, interoperate or be compatible with any specific mobile operating system platform or mobile device.

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". 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.

2. Content and Data Protection

The Data Processing and Protection data sheet (Data Sheet) provides information specific to the Cloud Service regarding the type of Content enabled to be processed, the processing activities involved, the data protection features, and specifics on retention and return of Content. Any details or clarifications and terms, including Client responsibilities, around use of the Cloud Service and data protection features, if any, are set forth in this section. There may be more than one Data Sheet applicable to Client's use of the Cloud Service based upon options selected by Client. The Data Sheet may only be available in English and not available in local language. Despite any practices of local law or custom, the parties agree that they understand English and it is an appropriate language regarding acquisition and use of the Cloud Services. The following Data Sheet(s) apply to the Cloud Service and its available options. Client acknowledges that i) IBM may modify Data Sheet(s) from time to time at IBM's sole discretion and ii) such modifications will supersede prior versions. The intent of any modification to Data Sheet(s) will be to i) improve or clarify existing commitments, ii) maintain alignment to current adopted standards and applicable laws, or iii) provide additional commitments. No modification to Data Sheet(s) will materially degrade the data protection of a Cloud Service.

Link(s) to the applicable Data Sheet(s):

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

IBM Trusteer Mobile Secure Browser

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

IBM Trusteer Pinpoint Assure

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=CF0C527046E011E8ADCBA344DE8FB657

IBM Trusteer Pinpoint Criminal Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489853624

IBM Trusteer Pinpoint Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=3D3DA0C0E5F711E5A3808DA17FABE9B1

IBM Trusteer Pinpoint Malware Detection

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489595035

IBM Trusteer Rapport

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402483908375

IBM Trusteer Pinpoint Verify

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

(The IBM Cloud Identity Verify data sheet reflects IBM Trusteer Pinpoint Verify)

Client is responsible to take necessary actions to order, enable, or use available data protection features for a Cloud Service and accepts responsibility for use of the Cloud Services if Client fails to take such actions, including meeting any data protection or other legal requirements regarding Content.

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and DPA Exhibit(s) apply and are referenced in as part of the Agreement, if and to the extent the European General Data Protection Regulation (EU/2016/679) (GDPR) applies to personal data contained in Content. The applicable Data Sheet(s) for this Cloud Service will serve as the DPA Exhibit(s). If the DPA applies, IBM's obligation to provide notice of changes to Subprocessors and Client's right to object to such changes will apply as set out in DPA.

2.1 EULA and Basis for Processing Data of Data Subjects

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

Unless otherwise agreed, and pursuant to the basis for processing that Client has independently established, Client authorizes IBM to provide the End User License Agreement available at https://www.trusteer.com/support/end-user-license-agreement to enable IBM to collect and process the information necessary for providing the Cloud Services.

2.2 Data Use

IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to your Content (Insights) or that otherwise identify Client. IBM may however use Content and other information (except for Insights) that results from Content in the course of providing the Cloud Service subject to removing personal identifiers; so that any personal data can no longer be attributed to a specific individual without the use of additional information. IBM will use such data only for research, testing, and offering development.

2.3 Data Processing and Storage

2.3.1 Additional Processing Location Information

For Trusteer Pinpoint Verify services, all hosting and processing locations are specified in the relevant Data Sheet.

For all other services provided through the Germany data center, IBM will limit processing of Personal Data to the country of the IBM contracting entity and to the following countries: Germany, Israel, Ireland, The Netherlands, and any additional countries listed in the applicable data sheet for IBM's Third Party Subprocessors.

For all other services provided through the Japan data center, IBM will limit processing of Personal Data to the country of the IBM contracting entity and to the following countries: Japan, Israel, Ireland, and any additional countries listed in the applicable data sheet for IBM's Third Party Subprocessors.

For all other services provided through the U.S. data center, IBM will limit processing of Personal Data to the country of the IBM contracting entity and to the following countries: U.S., Israel, Ireland, Singapore, Australia, and any additional countries listed in the applicable data sheet for IBM's Third Party Subprocessors.

IBM Trusteer support and account maintenance services may also be provided as needed, based on the availability of relevant IBM personnel, the location of the Client and the data center where the data is hosted.

2.3.2 Account Holder Data

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.

2.3.3 Integrated Solutions

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.

3. 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.

3.1 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.

3.2 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)
< 99.9%	2%
< 99.0%	5%
< 95.0%	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 Compensation 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:

$$\frac{\text{43,200 total minutes in a 30 day contracted month} - \text{230 minutes weighted Downtime} = \text{42,970 minutes}}{\text{43,200 total minutes}} = \text{2\% Availability credit for 99.4\% availability during the contracted month}$$

4. 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**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** and **IBM Trusteer Mobile Carrier Intelligence**. 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 IBM's software as a service support guide available at https://www.ibm.com/software/support/saas_support_guide.html.
- Clients can access Client Support Portal for notifications, documents, case reports and FAQs at: http://www-01.ibm.com/software/security/trusteer

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.ibm.com/software/security/trusteer/support/.
- For support options and details access IBM's software as a service support guide available at https://www.ibm.com/software/support/saas_support_guide.html.

5. Entitlement and Billing Information

5.1 Charge Metrics

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

- 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 Service. Sufficient entitlements must be obtained to cover each Engagement.
- 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.
- 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.
- 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 purpose of this Cloud Service, an Application is a single Business or Retail Application of the Client.
- API Call is a unit of measure by which the Cloud Service can be obtained. An API Call is the invocation of the Cloud Service through a programmable interface. Sufficient entitlements must be obtained to cover the total number of API Calls, rounded up to the nearest ten, during the measurement period specified in Client's PoE or Transaction Document.
- Connection is a unit of measure by which the Cloud Service can be obtained. A Connection is a link or association of a database, application, server, or any other type of device to the Cloud Service. Sufficient entitlements must be obtained to cover the total number of Connections which have been or are made to the Cloud Service during the measurement period specified in Client's PoE or Transaction Document.

  For the purpose of this Cloud Service, a Connection is a session or a flow in the Client's Application.

5.2 Overage Charges

If actual usage of the Cloud Service during the measurement period exceeds the entitlement specified in the PoE, an overage charge will be billed at the rate specified in the Transaction Document in the month following such overage.

5.3 Billing Frequency

Based on selected billing frequency, IBM will invoice Client the charges due at the beginning of the billing frequency term, except for overage and usage type of charges which will be invoiced in arrears.

6. 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. Renewals are subject to an annual price increase as specified in a quote. In the event the automatic renewal is after receipt of an IBM notice of a withdrawal of the Cloud Service, the renewal term will end the earlier of the end of the current renewal term or the announced withdrawal date.

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.

7. Additional Terms

7.1 General

The Client agrees IBM may publicly refer to Client as a subscriber to the Cloud Services in publicity or marketing communications.

Client may not use Cloud Services, alone or in combination with other services or products, in support of any of the following high risk activities: design, construction, control, or maintenance of nuclear facilities, mass transit systems, air traffic control systems, automotive control systems, weapons systems, or aircraft navigation or communications, or any other activity where failure of the Cloud Service could give rise to a material threat of death or serious personal injury.

7.2 Enabling Software

The Cloud Service requires the use of enabling software that Client downloads to Client systems to facilitate use of the Cloud Service. Client may use enabling software only in connection with use of the Cloud Service. Enabling software is provided "AS-IS".

7.3 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.