IBM Trusteer Pinpoint Detect

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

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. Trusteer Management Application (TMA) and Trustboard:

TMA is Trusteer's traditional management application that allows Clients to assess and classify alerts. Trustboard is a newer management application that is used primarily for research. Clients may choose to use either TMA or Trustboard at any one time. TMA and Trustboard are each 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. IBM Trusteer Pinpoint Detect and IBM Trusteer Pinpoint Verify are used as part of the TMA and Trustboard login.

b. Web Script and/or APIs:

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

A "Session" is an interaction between the Client's Application (Web or Mobile) and the Cloud Service that generates one or more real time risk assessments. A Session is measured from time of the beginning of the interaction until the end of the interaction. The end of an interaction is recorded when one of the following events occurs:

- Interaction is reset in the normal fashion of logging out of the application.
- Browser, application or tab is closed.
- Cookies are deleted.
- Timeout.

A Session can include any number of activities, such as: login, browsing, checkout, payment setup, and others as defined by the Client's Application. It is clarified that for purposes of this Cloud Service, one Connection (as defined below) is one Session.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 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. This Service can also be used for remote workforce accesses in order to assess risk from managed and unmanaged devices.

Premium support (as defined in the Technical Support section below) is included in this Cloud Service.

The service is available to be purchased by packs of 100 Eligible Participants or by packs of 100 Connections.

1.1.2 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.

1.1.3 IBM Trusteer Pinpoint Detect for Connections

This Cloud Service provides protection and aims to detect account takeover attempts and delivers risk / trust assessment scores of browsers and/or mobile devices (through the native browser of the Client mobile application) accessing a Business or Retail application. The solution uses various risk indicators analyzing the end user's device, connection and behavior and compares it with user history to identify suspicious usage.

The Cloud Service can consume connections from both Mobile and Web channels. IBM Trusteer Pinpoint Detect includes entitlement to the IBM Trusteer Mobile SDK, if relevant.

The Cloud Service is available to be purchased by packs of 100 Connections per year.

1.1.4 IBM Trusteer Pinpoint Detect Bundle

This Cloud Service bundle is powered by IBM Trusteer Pinpoint Detect, IBM Trusteer Mobile SDK and IBM Trusteer Rapport. This Cloud Service provides protection and aims to detect account takeover attempts and delivers risk / trust assessment scores of browsers and/or mobile devices (through the native browser of the Client mobile application) accessing a Business or Retail application. The solution uses various risk indicators analyzing the end user's device, connection and behavior and compares it with user history to identify suspicious usage.

The service is available to be purchased by Active User.

The Cloud Service can consume connections from both Mobile and Web channels. IBM Trusteer Pinpoint Detect includes access to the IBM Trusteer Mobile SDK.

IBM Trusteer Pinpoint Detect Bundle includes access to IBM Trusteer Rapport. Unless otherwise specified by IBM in writing, this access excludes Trusteer Splash and IBM Trusteer Rapport Mandatory Service.

IBM Trusteer Mobile SDK

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").

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.

The following provisions in this paragraph apply if the Cloud Services hereunder are provided by an entity other than International Business Machines Corporation, a New York corporation ("IBM Corporation"). The rights to the SDK and Redistributable hereunder are provided by IBM Corporation. IBM is acting as a distributor and delivering the SDK and Redistributable pursuant to this Agreement, and is responsible for enforcing the terms and fulfilling all obligations concerning the SDK and the Redistributable, and no right or cause of action hereunder is related in favor of Client against IBM Corporation. Client waives all claims and causes of action against IBM Corporation and agrees to look solely to IBM for any rights and remedies in connection with the SDK and the Redistributable.

IBM 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 offering includes:

a. Web Script:

   For access on a website for the purposes of accessing, testing or using the Cloud Service.

1.2 Optional Services

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

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Client Application refers to a Web Application and/or a Mobile Application. A Web Application groups all the functions offered to the Eligible Participants of the Client via several web pages, from a login or identification screen and monitored as a single Application in the Trusteer console (Trusteer Management Application). A Mobile Application groups together all the functions offered to the Eligible Participants of the Client via one software program that can be downloaded from an application store (store), from a login or identification screen and monitored as a single Application in the Trusteer console (Trusteer Management Application).

IBM Trusteer Pinpoint integration requires entitlement to IBM Trusteer Pinpoint Application for every Application.

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

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Client Application refers to a Web Application and/or a Mobile Application. A Web Application groups all the functions offered to the Eligible Participants of the Client via several web pages, from a login or identification screen and monitored as a single Application in the Trusteer console (Trusteer Management Application). A Mobile Application groups together all the functions offered to the Eligible Participants of the Client via one software program that can be downloaded from an application store (store), from a login or identification screen and monitored as a single Application in the Trusteer console (Trusteer Management Application).

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

1.2.3 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.

1.2.4 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.

1.2.5 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).

1.2.6 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.

1.2.7 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.

1.2.8 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:

   Clients may choose to use either TMA or Trustboard at any one time. Client (and unlimited number of its authorized personnel) can use either the TMA or Trustboard 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.

1.2.9 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:

Clients may choose to use either TMA or Trustboard at any one time. Client (and unlimited number of its authorized personnel) can use either the TMA or the Trustboard 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.

1.2.10 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 a 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. For the purpose of this Service Description, the 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 Service coverage. The 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.

1.2.11 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.

1.2.12 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.

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

- 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.

1.2.14 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 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.

1.2.15 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.

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

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

This Cloud Service enhances 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.

1.3 Acceleration Services

1.3.1 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.

1.3.2 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.

1.3.3 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.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below provide additional data protection information for the Cloud Services and its options regarding the types of Content that may be processed, the processing activities involved, the data protection features, and specifics on retention and return of Content. The DPA applies to personal data contained in Content, if and to the extent i) the European General Data Protection Regulation (EU/2016/679) (GDPR); or ii) other data protection laws identified at http://ibm.com/dpa/dpl apply.

It is clarified that the Data Sheets generally list all locations where IBM (including any third party subprocessors) hosts and processes Personal Data, without regard to the data center from which the services are deployed. For a list of hosting and processing locations that are specific to the data center from which the services are deployed, see Section 5.2 below (Additional Processing Location Information).

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 Mobile SDK

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

IBM Trusteer Rapport

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

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at https://www.ibm.com/support/home/pages/support-guide/.

Premium Support:

A Premium Support subscription is available for the Cloud Service at an additional charge and includes:

- 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/.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Engagement is a professional or training service related to the Cloud Services.

- Eligible Participant is an individual or entity eligible to participate in any service delivery program managed or tracked by the Cloud Services.
    - Active User is a unique person who accesses the Cloud Services in any manner directly or indirectly (for example, through a multiplexing program, device or application server) through any means.
- For IBM Trusteer Pinpoint Detect Bundle, an Active User is a unique person who accesses Cloud Services through any means at least once in the last 12 month period (prior to such time).
- Application is a uniquely named software program developed by or made available to access or used by the Cloud Services.
- API Call is the invocation of the Cloud Services through a programmable interface.
- Connection is a link or association of a database, application, server, or any other type of device which have been or are made available to the Cloud Services.

4.2 Remote Services Charges

A remote service will expire 90 days from purchase regardless of whether the remote service has been used.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at https://www.ibm.com/acs apply.

5.1 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://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA to enable IBM to collect and process the information necessary for providing the Cloud Services.

For IBM Trusteer Rapport Cloud Services, Client authorizes IBM, as the Sponsoring Enterprise's data processor, to use the Program to collect malware and malware artifacts, i.e., files related to malicious activity, or files related to unusual Program malfunction. IBM does not use the Program to target files with the end user's personal information; however, the files collected could contain personal data that has been obtained by the malware without the end user's permission. IBM will 1) promptly delete any files not relevant to such analysis, and 2) retain relevant files only for the duration of the analysis and in no event longer than three months.

5.2 Additional Processing Location Information

All hosting and processing of Personal Data, including by any third party subprocessors identified in the Data Sheet, will be conducted in the locations specified below:

For all services provided through the Germany data center, IBM will limit hosting and processing of Personal Data to the country of the IBM contracting entity and to the following countries: Germany, Israel, Ireland and The Netherlands.

For all services provided through the Japan data center, IBM will limit hosting and processing of Personal Data to the country of the IBM contracting entity and to the following countries: Japan, Israel and Ireland.

For all services provided through the U.S. data center, IBM will limit hosting and processing of Personal Data to the country of the IBM contracting entity and to the following countries: U.S., Israel, Ireland, Singapore and Australia.

In addition to the abovementioned locations, with respect to all services provided through the Germany, Japan and U.S. data centers, (1) support data may be hosted or processed in Germany and France by Salesforce.Com as a third party subprocessor of IBM and (2) for clients who opt to send data to Mobile Carrier Intelligence providers, Personal Data may hosted and processed in the countries of the applicable third party subprocessors as specified in the Data Sheet. Notwithstanding anything to the contrary in the Data Sheet, the third party subprocessors specified in clause (2) of the immediately preceding sentence might not be ISO 27001 or SOC2 compliant.

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.

5.3 Account Holder Data

For purposes of clarification, if there is more than one IBM customer affiliated with the Account Holder Client Software of a particular Account Holder (such IBM customers, "Affiliated Customers") and the services under this Service Description are provided by IBM to such Affiliated Customers through data centers in different regions, then the Account Holder's data may be processed in any and all locations associated with each such data center as specified in Section 5.2 above.

5.4 Integrated Solutions

For purposes of clarification, the various offerings under the Trusteer brand could constitute an integrated solution. Therefore, if Client terminates any of these Cloud Services, IBM may retain Client data for purposes of providing to Client the remaining Cloud Services under this Service Description as well as other Trusteer services pursuant to the service descriptions applicable to such other Trusteer services.

5.5 Enabling Software

The Cloud Service contains the following Enabling Software:

- IBM Rapport Agents

5.6 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).

5.7 Data Collected As Part of Deployment

Deployment of the Cloud Service may entail Client providing certain data to IBM. Such data must not include information that can identify or can be attributed to specific individuals. Further guidelines on data provided to IBM as part of deployment, are included in the Trusteer Deployment Guidelines to be provided to Client.

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content (Insights) or that otherwise identify Client. IBM will however use Content and other information that result from Content (except for Insights) as part of the Cloud Service for the purpose of improving the Cloud Service. IBM may also share threat identifiers and other security information embedded in Content for threat detection and protection purposes.