IBM Trusteer Pinpoint Assure

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 Assure is a security-rich layered solution that is purpose-built to help prevent individuals with fraudulent intent from using stolen identities, adding false data to real identities, or creating synthetic identities that can be used to make a guest transaction, open a brand-new account, or open a new digital account on behalf of an existing customer.

1.1 Offerings

1.1.1 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 Trusteer Management Application (TMA). IBM Trusteer Pinpoint Detect and IBM Trusteer Pinpoint Verify are used as part of the TMA login.

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

1.2 Optional Services

1.2.1 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.

1.2.2 IBM Trusteer Mobile Carrier Intelligence

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

This Cloud Service enhances IBM Trusteer Pinpoint Assure 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.

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 5.1 below (Additional Processing Location Information).

IBM Trusteer Assure

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

IBM Trusteer Mobile SDK

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

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/.

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:

- 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.
- Application is a uniquely named software program developed by or made available to access or used by the Cloud Services.

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 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.

5.2 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.

5.3 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.