IBM Financial Crimes Insight

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

1. Cloud Service

1.1 Offerings

The Client may select from the following available offerings:

1.1.1 IBM Financial Crimes Insight

This Cloud Service provides a common infrastructure and a common set of services upon which the Financial Crimes Insights offers are built. IBM Financial Crimes Insight provides the required integration between offerings allowing customers to take advantage of an integrated financial crimes set of offerings.

IBM Financial Crimes Insight is a required component that provides the Instance of the Cloud Service.

1.1.2 IBM Financial Crimes Insight Non-Production

This Cloud Service allows Client to access the IBM Financial Crimes Insight Non-Production functionality as a cloud offering.

1.1.3 IBM Financial Crimes Insight BYOL

This Cloud Service allows Client to access the IBM Financial Crimes Insight functionality as a cloud offering. Bring your own licenses (BYOL) offerings require the Client to have previously acquired appropriate license entitlements to the associated IBM Program. The IBM Program required by the IBM Financial Crimes Insight BYOL offering is IBM Cloud Pak for Data Financial Crimes Insight.

1.1.4 IBM Financial Crimes Insight Non-Production BYOL

This Cloud Service allows Client to access the IBM Financial Crimes Insight Non-Production functionality as a cloud offering. Bring your own licenses (BYOL) offerings require the Client to have previously acquired appropriate license entitlements to the associated IBM Program. The IBM Program required by the IBM Financial Crimes Insight Non-Production BYOL offering is IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment.

1.1.5 IBM Financial Crimes Insight for Entity Research Negative News API

This Cloud Service utilizes cognitive computing technology and advanced analytics to search, analyze and prioritize unstructured news and media for the purpose of uncovering potential financial crime risk of an entity by outputting a list of filtered and ranked articles. The offering is delivered as an API for organizations to call or embed into their workflows and processes.

1.1.6 IBM Financial Crimes Insight for Entity Research Enrichment API

This Cloud Service utilizes cognitive computing technology to aggregate data from structured sources which assists in helping organizations understand more about an entity, keeping entity or customer records up to date, and exposing potential financial crime risk of an entity. Entities could include customers, counter parties or suppliers. The offering is delivered as an API for organizations to call or embed into their workflows and processes.

1.2 Optional Services

In addition to subscribing to IBM Financial Crimes Insight or IBM Financial Crimes Insight Non-Production, Clients must also subscribe to one of the following Cloud Services:

1.2.1 IBM Financial Crimes Insight for Anti-Money Laundering

IBM Financial Crimes Insight for Anti-Money Laundering (FCI for AML) applies its layers of advanced analytics to monitor financial activity and help the Client identify the propensity of entities to launder money. Using demographic, behavioral, and relationship data, FCI for AML aids in the customer review process for known risks and may also increase risk coverage by providing explainable insights on hidden risks.

1.2.2 IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring

This Cloud Service utilizes data from historical cases, data aggregation of contextual evidence, and machine learning capabilities with the goal of streamlining the alert triage process, reducing false positives, accelerating disposition of the alert, and improving decision-making through a better understanding of entity risk. The service is an additional component that fits between the Client's institution existing transaction monitoring and case management systems.

1.2.3 IBM Financial Crimes Insight for Alert Triage – Transaction List Screening

This Cloud Service augments existing sanctions screening systems by analyzing alerted transactions using a configurable, extendable, API-driven pipeline. Transaction data is cleaned, parsed, and wrangled, then processed through heuristics and cognitive computing techniques. The results are used to score hits, identify false positives, and return informative, customizable insights.

1.2.4 IBM Financial Crimes Insight for Entity Research

This Cloud Service utilizes cognitive computing technology to screen, extract, and link relevant content from structured and unstructured data sources with the goal of improving the understanding of entities and / or the related risk of doing business with them, and reducing the time it takes to complete Know Your Customer (KYC) activities. The solution helps automate and standardize customer information research and analysis through aggregation of a variety of data sources. The goal of the service is an enhanced quality of KYC records in addition to an improved client experience through streamlined completion of research and due diligence activities.

The Client can select from the following entitlement options:

- IBM Financial Crimes Insight for Entity Research – Enterprise – each Event allows investigation of more than 5 related parties.
- IBM Financial Crimes Insight for Entity Research – Advanced – each Event allows investigation of up to 5 related parties.
- IBM Financial Crimes Insight for Entity Research – Basic – each Event allows investigation of up to 2 related parties.

A related party is any entity (organization or individual) that needs to be investigated as part of the review for a Parent Investigation as defined in Section 4.1. Typically, this can be authorized signers, officers, ultimate beneficial owners, parent or subsidiary organizations within the organization chart. For the avoidance of doubt, if a related party is an entity that requires investigation of its individual or associated members, then each individual or associated member also counts as a related party.

1.2.5 IBM Financial Crimes Insight for Entity Research with Material Change

This Cloud Service utilizes cognitive computing technology to screen, extract, and link relevant content from structured and unstructured data sources with the goal of improving the understanding of entities and / or the related risk of doing business with them, and reducing the time it takes to complete Know Your Customer (KYC) activities. The solution helps automate and standardize customer information research and analysis through aggregation of a variety of data sources. The goal of the service is an enhanced quality of KYC records in addition to an improved client experience through streamlined completion of research and due diligence activities. This includes the Material Change functionality, which allows for monitoring entities on a schedule for any material differences and alert the analyst to review.

The Client can select from the following entitlement options:

- IBM Financial Crimes Insight for Entity Research – Enterprise – each Event allows investigation of more than 5 related parties.
- IBM Financial Crimes Insight for Entity Research – Advanced – each Event allows investigation of up to 5 related parties.
- IBM Financial Crimes Insight for Entity Research – Basic – each Event allows investigation of up to 2 related parties.

A related party is any entity (organization or individual) that needs to be investigated as part of the review for a Parent Investigation as defined in Section 4.1. Typically, this can be authorized signers, officers, ultimate beneficial owners, parent or subsidiary organizations within the organization chart. For the avoidance of doubt, if a related party is an entity that requires investigation of its individual or associated members, then each individual or associated member also counts as a related party.

1.2.6 IBM Financial Crimes Insight for Claims Fraud – Property and Casualty

This Cloud Service helps organizations analyze data to detect risk resulting from fraudulent claims that are submitted by their customers, by medical providers or other entities, and to manage the full investigation life cycle, and report on outcomes.

1.2.7 IBM Financial Crimes Insight for Claims Fraud – Investigation

This Cloud Service helps organizations manage the full investigation lifecycle of suspicious activities and potential fraud.

1.2.8 IBM Electronic Communication Surveillance Analytics on Cloud

This Cloud Service is a tool to help financial services institutions effectively analyze and monitor employees' interaction data across multiple channels in order to detect various patterns of suspicious communications. The tool helps detect various patterns of rogue behavior related to market abuse and manipulation. The tool leverages natural language processing capability to understand text information and to distinguish ambiguous terms based on context. The tool also uses sentiment and emotion analysis capabilities which can be used to analyze communications. These capabilities are not meant to be used to, nor do they, infer personality traits of individuals. This analysis feeds into the overall reasoning engine which helps in linking various insights together and providing risk estimation to compliance officers.

1.2.9 IBM Voice Surveillance Analytics on Cloud

This Cloud Service is a tool to help financial services institutions analyze and monitor employees' voice communication across multiple channels to detect suspicious activity. The tool uses speech-to-text technology to convert human voice into written word by leveraging machine learning to detect grammar and language structure. It links the speech-to-text output with the rich meta-data generated by the telephony system and applies speaker diarisation to the text in order to allow for quick and easy search and replay of voice conversations of interest. The speech-to-text output along with the metadata is made available to Client in a well-defined format. As additional options, the tool can use natural language processing to extract semantic meta-data from content and linguistic analysis to detect topics, tones, sentiment and emotion. These capabilities are not meant to be used to, nor do they, infer personality traits of individuals. All speech to text conversion is done "in memory" to reduce storage of duplicate files and transcripts and no voice data is stored in the Cloud after the processing.

1.2.10 IBM Complaints Analytics on Cloud

This Cloud Service enables organizations to identify, aggregate and categorize complaints, allegations, and other activity. It provides insights on emerging issues to address increasing regulatory expectations. The tool leverages advanced analytics to identify and analyze complaints that would otherwise be missed by traditional systems. It can ingest structured and unstructured data such as Client data, emails, service notes, social media complaints, and voice recordings. It then uses cognitive capabilities to aggregate and enrich complaints data to identify systemic risks. It also applies dynamic segmentation and time series profiling to monitor and anticipate changes and trends.

In order to use IBM Complaints Analytics on Cloud, Client must also subscribe to either IBM Electronic Communication Surveillance Analytics on Cloud or IBM Voice Surveillance Analytics on Cloud.

1.2.11 IBM Electronic Communication Surveillance Analytics on Cloud BYOL

This Cloud Service allows Client to access the IBM Electronic Communication Surveillance Analytics on Cloud functionality as a cloud offering. Bring your own licenses (BYOL) offerings require the Client to have previously acquired appropriate license entitlements to the associated IBM Program. The IBM Program required by the IBM Electronic Communication Surveillance Analytics on Cloud BYOL offering is IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication.

1.2.12 IBM Voice Surveillance Analytics on Cloud BYOL

This Cloud Service allows Client to access IBM Voice Surveillance Analytics on Cloud functionality as a cloud offering. Bring your own licenses (BYOL) offerings require the Client to have previously acquired appropriate license entitlements to the associated IBM Program. The IBM Program required by the IBM Voice Surveillance Analytics on Cloud BYOL offering is IBM Financial Crimes Insight for Conduct Surveillance Software – Voice.

1.2.13 IBM Complaints Analytics on Cloud BYOL

This Cloud Service allows Client to access the IBM Complaints Analytics functionality as a cloud offering. Bring your own licenses (BYOL) offerings require the Client to have previously acquired appropriate license entitlements to the associated IBM Program. The IBM Program required by the IBM Complaints Analytics on Cloud BYOL offering is IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics.

1.3 Acceleration Services

1.3.1 IBM Financial Crimes Insight Set-up

The following set-up services are required in order for Client to be provisioned for use of the corresponding Cloud Service:

- IBM Financial Crimes Insight for Anti-Money Laundering Set-up
- IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring Set-up
- IBM Financial Crimes Insight for Alert Triage – Transaction List Screening Set-up
- IBM Financial Crimes Insight for Entity Research – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research – Advanced Set-up
- IBM Financial Crimes Insight for Entity Research – Basic Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Advanced Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Basic Set-up
- IBM Financial Crimes Insight for Entity Research Negative News API Set-up
- IBM Financial Crimes Insight for Entity Research Enrichment API Set-up
- IBM Financial Crimes Insight for Claims Fraud – Property and Casualty Set-up
- IBM Financial Crimes Insight for Claims Fraud – Investigation Set-up
- IBM Surveillance Insight for Financial Services on Cloud Set-up

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://www.ibm.com/dpa/dpl apply.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=14BD7780D65B11E99EAFC519926DF897

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%

Availability	Credit (% of monthly subscription fee*)
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:

- Engagement is a professional or training service related to the Cloud Services.
- Instance is each access to specific configuration of the Cloud Services.
- Event is an occurrence of a specific event that is processed by or related to the use of the Cloud Services.
    - For IBM Financial Crimes Insight for Anti-Money Laundering, an Event is 10 million financial transactions in one calendar month.
    - For IBM Financial Crimes Insight for Claims Fraud – Property and Casualty and IBM Financial Crimes Insight for Claims – Investigation, an Event is an occurrence of a Claim. Claim is a set of instructions related to a formal request to an organization for coverage or compensation for a covered loss or event.
    - For IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring, an Event is an individual alert / event ingested into the Cloud Service from the originating system in one calendar month. Typically, an originating source system is a transaction monitoring system or a case management system.
    - For IBM Financial Crimes Insight for Alert Triage – Transaction List Screening, an Event is up to 1,000 individual alerts ingested into the Cloud Service from the originating system in one calendar month. Typically, an originating source system is a transaction monitoring system or a case management system.
    - For IBM Financial Crimes Insight for Entity Research and IBM Financial Crimes Insight for Entity Research with Material Change, an Event is any parent investigation processed by the Cloud Service, including identical repeated searches, in one calendar month. A parent investigation is any record which is not linked as a child to another investigation. A child is a related party (as described in section 1.2.5) that is not otherwise subject to a parent investigation.
- Eligible Participant is an individual or entity eligible to participate in any service delivery program managed or tracked by the Cloud Services.
- Item is an occurrence of a specific item that is managed by, processed by, or related to the use of the Cloud Service.
    - For IBM Voice Surveillance Analytics on Cloud, an Item is one hour of Voice Stream processed by the Cloud Service in a calendar day. A Voice Stream is a capture of audio communication in either real-time or recorded format.
- API Call is the invocation of the Cloud Services through a programmable interface.
- Entity ID is a unique identifier for any entity identified within 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 Supporting Programs

IBM Financial Crimes Insight and IBM Financial Crimes Insight Non-Production includes access to certain programs ("Supporting Programs") that are deployed in the cloud environment. Client may use these Supporting Programs only for the purpose of countering or otherwise taking action intended to identify and/or inhibit fraud, financial crimes, and improper payments.

5.1.1 Use Limitations – Specific to Certain Supporting Programs

The following Supporting Programs are available under the following restrictions:

- IBM Watson Studio – Entitlement: 5 Concurrent Users
- IBM Watson Machine Learning – Entitlement: 50 Models
- IBM Openscale – Entitlement: 50 Models
- IBM SPSS Modeler Premium – Entitlement: 4 Authorized Users
- IBM SPSS Statistics Standard – Entitlement: 4 Authorized Users
- Watson Explorer Advanced Edition – Entitlement: per X Gigabytes as defined below.

  Client is permitted to analyze:

  - all Content stored in the Cloud Service's repository for use with Non-Analytics Collections;
  - up to 10 Gigabytes of Content not stored in the Cloud Service's repository for use with Non-Analytics Collections.
  - 100 Gigabytes of Content stored in the Cloud Service's repository for use with Analytics Collections.

    Analytics Collections refer to collections created in the Watson Explorer annotation Administration Console, or created in the Watson Explorer Content Analytics Administration Console or via the API as type "Content Analytics" or "Analytics".

    Non-Analytics Collections include all other content analyzed by the Program Cloud Service.
- IBM InfoSphere DataStage – IBM InfoSphere DataStage and QualityStage Designer Entitlement: 2 Authorized Users
- IBM Operational Decision Manager – Entitlement: 1 million Monthly Rules Decisions and 1 thousand Monthly Managed Decision Artifacts

Entitlement Definitions

a. Concurrent User is a person who is accessing the Supporting Program at any particular point in time. Regardless of whether the person is simultaneously accessing the Supporting Program multiple times, the person counts only as a single Concurrent User.

b. Model is a mathematical model or algorithm concerning the underlying data or data-generation process used for simulating, explaining, and making predictions in the Supporting Program.

c. Authorized User is a unique user authorized to access the Supporting Program in any manner directly or indirectly (for example, through a multiplexing program, device or application server) through any means.

d. Gigabyte (GB) is 2 to the 30th power bytes of data processed by, analyzed, used, stored, or configured in the Supporting Program.

e. Monthly Rules Decisions is the outcome of invoking a ruleset from a rule execution server executed or processed by the Supporting Program in any calendar month.

f. Monthly Managed Decision Artifacts is an object managed by the Supporting Program in any calendar month.

5.2 Terms applicable to IBM Financial Crimes Insight BYOL

Bring your own licenses (BYOL) offerings require the Client to have previously acquired appropriate license entitlements to the associated IBM Program identified in the table below. Client's entitlements to

the BYOL SaaS cannot exceed Client's entitlements to the associated IBM Program, in the ratios specified below.

The BYOL offering does not include Subscription and Support (S&S) for the associated IBM Program. Client represents they have acquired the applicable (1) license entitlements and (2) S&S for the associated IBM Program. During the subscription period of the BYOL offering, Client must maintain current S&S for the IBM Program entitlements used in conjunction with the BYOL offering entitlements. In the event either Client's license to use the associated IBM Program or Client's S&S for the associated IBM program is terminated, Client's right to use the BYOL offering will terminate.

Client may continue to use the entitlements to the associated IBM program that are applied to usage of the BYOL offering to deploy the associated IBM program concurrently with Client's use of the BYOL offering for the following period (the "Concurrent Usage period"): for Clients with a subscription term of less than three (3) years, no longer than ninety (90) days after the start of the Client's initial subscription to the BYOL offering; for Clients with a subscription term of three (3) years or more, no longer than one (1) year after the start of the Client's initial subscription to the BYOL offering. After the end of the Concurrent Usage period, for the duration of Client's use of the BYOL offering, Client's entitlements to the associated IBM program applied to usage of the BYOL offering are suspended and Client may no longer use those entitlements to deploy the associated IBM program (subject to any stated exceptions).

The table below outlines the ratio of entitlements for the associated IBM Program required for usage of the BYOL offering under the stated corresponding entitlement. Once Client has obtained the BYOL offering and for the duration of Client's use of the BYOL offering, Client's entitlements to the associated IBM Program applied to usage of the BYOL offering are suspended and Client may no longer use those entitlements to deploy the associated IBM Program (subject to any stated exceptions).

Associated IBM Program	BYOL Offering	Ratio n/m*
IBM Cloud Pak for Data Financial Crimes Insight	IBM Financial Crimes Insight BYOL	Ratio: 1 Install / 1 Instance
IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment	IBM Financial Crimes Insight Non-Production BYOL	Ratio: 1 Install / 1 Instance
IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication	IBM Electronic Communication Surveillance Analytics on Cloud BYOL	Cumulative Ratios: Tier 1 (1-100 RVUs): ● 1 RVU / 1 Eligible Participant Tier 2 (101-235 RVUs): ● 0.9 RVUs / 1 Eligible Participant Tier 3 (236-435 RVUs): ● 0.8 RVUs / 1 Eligible Participant Tier 4 (436-585 RVUs): ● 0.6 RVUs / 1 Eligible Participant Tier 5 (586-835 RVUs): ● 0.5 RVUs / 1 Eligible Participant Tier 6 (836-1,135 RVUs): ● 0.4 RVUs / 1 Eligible Participant Tier 7 (1,136+ RVUs): ● 0.3 RVUs / 1 Eligible Participant
IBM Financial Crimes Insight for Conduct Surveillance Software – Voice	IBM Voice Surveillance Analytics on Cloud BYOL	Cumulative Ratios: Tier 1 (1-100 RVUs): ● 1 RVU / 1 Item Tier 2 (101-235 RVUs): ● 0.9 RVUs / 1 item Tier 3 (236-435 RVUs): ● 0.8 RVUs / 1 Item Tier 4 (436-585 RVUs): ● 0.6 RVUs / 1 Item Tier 5 (586-835 RVUs): ● 0.5 RVUs / 1 Item Tier 6 (836-1,135 RVUs): ● 0.4 RVUs / 1 Item Tier 7 (1,136+ RVUs): ● 0.3 RVUs / 1 Item

Associated IBM Program	BYOL Offering	Ratio n/m*
IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics	IBM Complaints Analytics on Cloud BYOL	Cumulative Ratios: Tier 1 (1-100 RVUs): ● 5 RVU / 1 Entity ID Tier 2 (101-235 RVUs): ● 4.5 RVUs / 1 Entity ID Tier 3 (236-435 RVUs): ● 4 RVUs / 1 Entity ID Tier 4 (436-585 RVUs): ● 3 RVUs / 1 Entity ID Tier 5 (586-835 RVUs): ● 2.5 RVUs / 1 Entity ID Tier 6 (836-1,135 RVUs): ● 2 RVUs / 1 Entity ID Tier 7 (1,136+ RVUs): ● 1.5 RVUs / 1 Entity ID

* "Ratio n/m" means that for every ('n') entitlements of the indicated metric for the associated IBM program, Client may apply those entitlements into the specified number ('m') entitlements of the indicated metric for the BYOL offering. If conversion from an Associated IBM Program to a BYOL Offering results in a non-integer, round up to the nearest integer.

Example 1:

710 RVUs to Eligible Participant (EPS)

(Applicable to IBM Trade Surveillance Analytics and IBM Electronic Communication Surveillance Analytics)

Tier 1: if 710>100, then 100/1 = 100 EPS

Tier 2: if 710>235, then (235-100)/.9 = +150 EPS

Tier 3: if 710>435, then (435-235)/.8 = +250 EPS

Tier 4: if 710>585, then (585-435)/.6 = +250 EPS

Tier 5: if 710>835 → no so then (710-585)/.5 = +250 EPS

Total EPS: 100 + 150 + 250 + 250 + 250 = 1000 EPS

Example 2:

250 RVUs (pack of 100,000) to Entity ID (pack of 500,000)

(Applicable to IBM Complaints Analytics)

Tier 1: if 250>100, then 100/5 = 20 Entity ID

Tier 2: if 250>235, then (235-100)/4.5 = +30 Entity ID

Tier 3: if 250>435 → no so then (250-235)/4 = +3.75 Entity ID

Total EPS: 20 + 30 + 3.75 = 53.75 Entity ID, rounded up to 54 Entity ID

Check: 250 RVU = 269 Resources * 100,000 Pack Size On Prem / 500,000 Pack Size SaaS = 53.75, rounded up to 54 Entity ID

5.3 Third Party Content

Client acknowledges that the search results obtained and referenced in the reports generated as part of the Cloud Services described herein ("Search Results") may include data or Content owned by third parties and that IBM is not selling or providing any license or any other rights to such Search Results or Content. Client agrees that it is solely responsible for obtaining and shall obtain before using any of the Cloud Services described herein any and all such licenses, rights and permissions from the applicable third parties as are necessary under the laws applicable to such Search Results for Client, or IBM on Client's behalf, to use, hold, retain, process or reproduce or adapt such Search Results. Client authorizes IBM and its affiliates, and contractors of either to access, reproduce, adapt or otherwise process on Client's behalf, the third party data sources (including any data or Content contained in or obtained from the Search Results) in connection with the Cloud Services herein. For the purposes of this Section 5.3, Content consists of any copyright work, data, images, software or information that Client or its authorized users provides, authorizes access to, or inputs into the Cloud Service.

5.4 Cloud Service Expiration

Before expiration or termination of the Cloud Service, Client can use any of the provided reporting or export features of the Cloud Service to extract data. Custom data extraction services are available under a separate agreement.

Upon receiving a support request from Client within 30 days of the Cloud Service expiration or termination date, IBM will return to Client an electronic copy of Client's content in the native application format.