GSMA FRAUD INTELLIGENCE SERVICE
TERMS OF USE

Effective date: 15 January 2021

These terms of use govern your agreement with GSMA for use of the GSMA Fraud Intelligence Service. Please read these terms of use carefully before you register or use GSMA Fraud Intelligence Service. These terms of use tell you how the GSMA Fraud Intelligence Service works, how our agreement may be updated or terminated, and other important information.

By registering, using or accessing GSMA Fraud Intelligence Service, you agree to these terms of use, as updated from time to time in accordance with clause 18. If you think that there is a mistake in these terms, please contact GSMA at FIShelpdesk@gsma.com.

INTRODUCTION:

(A) The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.

(B) The GSMA has identified a need for a fraud deterrent and security risk database service to support the mobile network operators, mobile virtual network operators, their international roaming partners and other providers of communication services, when it comes to the roaming and interconnect fraud prevention.

(C) The GSMA has therefore established the GSMA Fraud Intelligence Service to provide a central global database and exchange platform to assist MNOs and MVNOs in analysing fraud related incidents efficiently and with more accuracy by providing High Risk Numbers (HRN) information along with analysis tools and other relevant information to assist users in mitigating telecommunications crime, fraud and security risks.

(D) This Agreement sets out the terms and conditions on which GSMA will provide access to, and you may use, the GSMA Fraud Intelligence Service.

YOU AGREE THAT:

1. DEFINITIONS

1.1 In this Agreement, unless the context indicates otherwise:

Affiliate means any subsidiary or holding company of an entity, any subsidiary of any of its holding companies and any partnership, company or undertaking (whether incorporated or unincorporated) in which that entity has the majority of the voting rights or economic interest.

Agreement means these GSMA Fraud Intelligence Service Terms of Use and your Order Form.

Contributor means a person who has contributed Submissions to the Fraud Intelligence Service by any means.

Data Protection Laws means all legislation, principles, codes and policies in any relevant jurisdiction applicable to the collection, use, disclosure, Processing, transfer or granting of access rights to any Personal Data, including, without limitation, any applicable local laws, and any related decisions or guidelines and subsequent legislation of a similar nature, and the GDPR.

Eligible User means (i) an MNO; or (ii) an MVNO managing its own roaming agreements.

Fees means the annual fees payable for use of the Service in accordance with clause 7, as set out in your

Order Form.

FF.21 means the GSMA Fraud Manual, as updated from time to time by GSMA and notified to you by GSMA by email.

Fraud Intelligence Data means the information contained in the Fraud Intelligence Service, being the HRN Data, IR.21 Data, other categories of information set out in Schedule 2, and any other data GSMA may add to the Platform in the future.

GDPR means the General Data Protection Regulation (Regulation (EU) 2016/679).

GSMA means GSMA Ltd., a Georgia not-for-profit corporation and a wholly-owned subsidiary of the GSM Association, with an office at 165 Ottley Drive, Suite 150, Atlanta, Georgia 30324, U.S.

GSMA Fraud Intelligence Service means the cyber threat and fraud intelligence services provided via the Platform, as further described in Schedule 1.

GSMA Group means GSMA, GSM Association, and their Affiliates.

High Risk Numbers Service means the GSMA service to receive, store and distribute HRN Data, being a subset of the GSMA Fraud Intelligence Services.

HRN Data means the following "High Risk Numbers" data:
(i) telephone number;
(ii) a telephone number range;
(iii) MSRN; and/or
(iv) MSRN range;
with associated Fraud Labels, Status and Comments, as described in Schedule 2, reported to GSMA as being associated with fraudulent or nuisance traffic as set out in FF.21.

Intellectual Property Rights means copyrights, database rights, patents, utility models, know-how, registered and unregistered design rights, trade marks, confidential information, trade secrets, and other intellectual property, in each case whether registered or unregistered, and any rights to apply for the foregoing, which may subsist anywhere in the world.

IR.21 means the IR.21 GSM Association Roaming Database, Structure and Updating Procedures permanent reference document, as updated from time to time by GSMA and notified to you by GSMA by email.

IR.21 Data means the telephone number or Mobile Station ISDN Number (MSISDN) ranges, Mobile Station Roaming Number (MSRN) ranges, International Mobile Subscriber Identity (IMSI) ranges, Internet Protocol (IP) address ranges and other data associated with an operator accessed from RAEX or other available sources, as further described in Schedule 2.

MNO means a mobile network operator, being any person that provides publicly available mobile telecommunications services (and is licensed to do so by the appropriate governmental or regulatory authorities) on a wholesale or retail basis through the use of (i) a technology within the GSM family of technology standards, as in effect from time to time, including without limitation GSM, GPRS, EDGE, HSCSD, 3GSM/UMTS, HSPA, UMTS-TDD, W-CDMA, FOMA,LTE and 5G; (ii) a technology within the CDMA family of standards, as in effect from time to time, including without limitation 1xRTT, EV-DO and EV-DV; (iii) TD-SCDMA technology; or (iv) any technology classified as an IMT-2000 technology by the ITU.

MSRN means Mobile Station Roaming Number, being a number allocated to a subscriber for routing purposes.

MVNO means a mobile virtual network operator, being any person providing mobile telecommunications services like those of an MNO but not itself owning all infrastructure necessary to provide the telecommunications services.

Order Form means the order form in the format provided by GSMA and agreed in writing by the parties (whether in electronic or physical format).

Permitted Affiliate(s) means the Affiliates listed in your Order Form, if any. Note that additional fees may apply per Permitted Affiliate.

Personal Data has the meanings given in the GDPR and the other Data Protection Laws, and includes "Personal Information" and "Personally Identifiable Information" as those terms are defined in the applicable Data Protection Laws. For the avoidance of doubt, device unique identifiers, telephone numbers, including Mobile Station ISDN Numbers (MSISDN), Mobile Station Roaming Numbers (MSRN) or ranges, Short Codes (Short Numbers), contact details, descriptive fraud comments and any information relating or attributed to the foregoing shall be treated as Personal Data for the purposes of this Agreement.

Platform means (i) the web platform for accessing and using the GSMA Fraud Intelligence Service as a user interface located via www.gsma.com/services; and (ii) where applicable, the API access mechanism.

Policies means IR.21, FF.21, and any other relevant GSMA policy and permanent reference documents, relating to GSMA Fraud Intelligence Service, each as updated from time to time by GSMA and notified to you by GSMA from time to time by email.

Process means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing has the corresponding meaning.

Purpose means mitigating telecommunications crime and fraud.

RAEX means the Roaming Agreement Exchange, the GSMA IR.21 database as specified in IR.21.

Retention Period has the meaning given in clause 10.5.

Standard Contractual Clauses means the Standard Contractual Clauses for the Transfer of Personal Data from the Community to Third Countries (Controller to Controller transfers) as set out in the Annex to 2004/915/EC: Commission Decision of 27 December 2004.

Subcontractor means a third party supplier contracted to provide goods or services, for example, IT, hardware, software, telecommunications and SaaS providers.

Submission means HRN Data submitted to the GSMA Fraud Intelligence Service (whether via the GSMA High Risk Numbers Service or otherwise) by a user. Any HRN Data previously provided to GSMA (whether via email or Fraud and Security Group Processes) will be treated as a Submission for the purposes of all GSMA Fraud Intelligence Services.

Subscription means an annual subscription for using the GSMA Fraud Intelligence Services.

Tax means any tax, levy or duty payable in relation to the Fees or otherwise in relation to this Agreement.

Term means the term of this Agreement, as set out in clause 14.

User means any user of the Platform, including you and the Contributors, as the context requires.

you or **your** means you as the counterparty to this Agreement, being a User approved by GSMA to use the GSMA Fraud Intelligence Service, as further set out in clause 2 (Registration Requirements and Process).

1.2 In this Agreement, unless the context indicates otherwise:

(a) clause and other headings are for ease of reference only and will not affect this Agreement's interpretation;

(b) any obligation not to do anything includes an obligation not to suffer, permit or cause that thing to be done;

(c) references to a “person” include an individual, company, corporation, partnership, firm, joint venture, association, trust, unincorporated body of persons, governmental or other regulatory body, authority or entity, in each case whether or not having a separate legal identity;

(d) the term “includes” or “including” (or any similar expression) is deemed to be followed by the words "without limitation"; and

(e) references to any document are references to that document as modified or replaced from time to time.

2. REGISTRATION AND EXISTING FRAUD INTELLIGENCE CONTRIBUTORS

2.1 Use of the GSMA Fraud Intelligence Service is subject to your prior completion of all required applications forms and provision of any related information reasonably requested by GSMA in relation to the GSMA Fraud Intelligence Service. In order to register for and to use the GSMA Fraud Intelligence Service, you must be an Eligible User. GSMA will be entitled, in its sole discretion, to reject any application. In the event an application is not accepted, any relevant Fees paid in advance will be refunded in full.

2.2 By registering to access the GSMA Fraud Intelligence Service, you agree that, if you are a contributor of information to the GSMA RAEX database or the High Risk Range List, this information may be provided by GSMA to other Users of the Fraud Intelligence Service in compliance with IR.21 where applicable. Please contact GSMA at FIShelpdesk@gsma.com if you have any questions about this.

3. ACCESSING GSMA FRAUD INTELLIGENCE SERVICES

3.1 Subject to the terms set out in this Agreement, you may access the Platform during the Term to:

(a) access and receive Fraud Intelligence Data from the Platform, subject to the requirements in clause4; and

(b) make Submissions to the GSMA Fraud Intelligence Service, subject to the terms and requirements in clause 5.

3.2 You will NOT:

(a) provide access to the Platform or the Fraud Intelligence Data to any other person or entity (including any Affiliate), except as permitted by clauses 4.6 (Subcontractors) and 12 (Permitted Affiliates), where applicable;

(b) act as an agent for, or otherwise on behalf of, any other person or entity in making Submissions to the GSMA Fraud Intelligence Service (except as permitted by clause 12 (Permitted Affiliates), where applicable);

(c) resell access to the GSMA Fraud Intelligence Service, the Fraud Intelligence Data, the Platform, or the right to make Submissions.

4. USING FRAUD INTELLIGENCE DATA

4.1 You may access the Fraud Intelligence Data via the Platform, in accordance with the access instructions provided by GSMA to you (as updated from time to time and notified to you by email by GSMA).

4.2 You may use the Fraud Intelligence Data solely for the Purpose. Subject to clause 4.7, you must keep confidential the Fraud Intelligence Data, and you may not provide the Fraud Intelligence Data to any other person, individual, organisations or groups, either directly or via third parties. Please contact GSMA with any queries on how Fraud Intelligence Data may be disclosed.

4.3 Fraud Intelligence Data can change at any time based on Contributor input. GSMA takes no responsibility for any variance or the effects of any variance between Fraud Intelligence Data supplied through the Platform and your or Contributors' historical records.

4.4 Following termination or expiry of this Agreement, subject to the confidentiality requirements set out in this Agreement, you may retain Fraud Intelligence Data received under this Agreement solely to the extent and for the duration required by law.

4.5 You must promptly notify GSMA of any third party claim or complaint that You become aware of in relation to any of the Fraud Intelligence Data.

4.6 You may authorise your Subcontractors to access and use the Fraud Intelligence Services for and on behalf of you solely for the purposes of providing services to you, provided that Subcontractors must comply with all restrictions and obligations of yours under this Agreement. You are responsible for the acts and omissions of each of your Subcontractors as if they were your acts and omissions. This Agreement does not create a contractual relationship between the GSMA and any Subcontractor, who have no right to enforce any term of, or any rights in relation to, this Agreement.

4.7 Notwithstanding clauses 4.2 and subject to clause 9, you can disclose Fraud Intelligence Data, (i.e. a telephone number), as required to a MNO or MVNO solely as required in order to discuss a specific suspected fraud case for your own or the recipient MNO/MVNO's internal purposes. You may not disclose substantial portions of Fraud Intelligence Data, and may not disclose Fraud Intelligence Data in a manner that replicates, relicenses or resells the Fraud Intelligence Services or any part thereof or is otherwise deemed by GSMA as a HRN Data or IR.21 Data distribution service.

5. SUBMITTING FRAUD INTELLIGENCE DATA

5.1 You will be provided with access to make Submissions via the Platform in accordance with the Policies. For each Submission, you must:

(a) only submit telephone numbers that have been identified as sources of fraud, nuisance calls and any other form of recognised unwanted calls. You may use FF.21, bespoke or GSMA defined fraud types to label submitted numbers;

(b) ensure that (i) any data subject to whom the Personal Data contained within the Submission relates has provided their consent (as defined by GDPR); or (ii) it is otherwise lawful to make the Submission in accordance with the Data Protection Laws;

(c) use best efforts to ensure that each Submission is accurate, timely, current, and complete;

(d) respond in a timely fashion to inquiries from other Contributors and users of the GSMA Fraud Intelligence Service, regarding your Submissions;

(e) promptly remove/update Submissions as required to correct any inaccurate Submissions;

(f) make Submissions utilizing the format set out in Fraud Intelligence Service User Guide and in accordance with GSMA's reasonable directions from time to time; and

(g) comply with the Policies.

5.2 Acknowledging that users of the GSMA Fraud Intelligence Service may receive and use updated Fraud Intelligence Data information hourly (or more frequently), you must make Submissions and relevant updates as timely as reasonably possible. Without limiting the foregoing, except where GSMA provides prior written approval, you will not make any new Submission based upon activity (any act, omission or discovery) which takes place (i) prior to the Access Date; or (ii) more than 18 months prior to the date of the Submission.

5.3 You will promptly notify GSMA of any third party claim or complaint that You become aware of in relation to any of your Submissions.

6. USE OF CREDENTIALS AND PASSWORDS

6.1 If your application is approved by GSMA (where required), you will be issued with unique user ID(s) and password(s) ("**User Credentials**"). Your User Credentials may only be used by the named individual user. You must ensure that the User Credentials are not shared outside of your organization or misused in any way. You must keep User Credentials confidential and secure. You will be responsible for all use of, and activity associated with, your User Credentials (whether such use or activity is authorized by you or not). You must immediately notify GSMA in the event of suspected or actual loss, theft, unauthorized access or hacking of your User Credentials.

6.2 You will NOT:

(a) circumvent, or attempt to circumvent, any data security measures employed by GSMA;

(b) use, or cause to be used, any automated program or script, or other functionality or technique, which conceals, or is misleading or deceptive as to, your identity, or use of, or activity on, the Platform; or

(c) attempt to interfere with the Platform by any means, including by hacking the GSMA systems or servers, submitting a virus, overloading, or crashing the GSMA sites or systems.

6.3 GSMA retains the right to remove, disallow or cancel User Credentials in its sole and absolute discretion. GSMA may, without any prior notice to you, terminate, cancel or suspend your User Credentials if, in GSMA's sole and absolute discretion, GSMA determines that your use of the User Credentials would or may constitute or cause (or has constituted or caused) a breach, contravention, or infringement of this Agreement, any rights of any third party or any applicable laws, rules or regulations.

6.4 GSMA will treat any user contact details provided by you in accordance with applicable data privacy laws, including the Privacy Policy available at https://www.gsma.com/aboutus/legal/privacy.

7. FEES AND PAYMENT

7.1 Fees are payable to GSMA annually in advance, prior to accessing and using GSMA Fraud Intelligence Service. Fees are payable:

(a) within 30 days of invoice by GSMA; or

(b) prior to the expiry date of your then-current Subscription if you are renewing a Subscription.

Your Subscription commences on the date that your payment and application has been processed by GSMA. You should allow up to 30 days for the processing of your application and payment prior to the commencement of your Subscription. No refunds or discounts are provided due to any delay in processing your application or payment.

7.2 Invoices will be generated following your successful registration and agreement to this Agreement, and then annually in advance of your Subscription renewing. Invoices will be delivered by email to your billing contact provided in the registration process.

7.3 Payment of invoices must be made by bank/wire transfer in accordance with the invoice instructions. Please note that payment by bank transfer can take 5 to 10 working days for the money to reach GSMA. Your User Credentials for the Platform will not be provided until the invoice payment has been received to the GSMA account indicated on the invoice. You will be sent a notification email when the payment has been received.

7.4 Upon the expiration of the Subscription, your Subscription will automatically renew for successive one year Subscriptions (each a "**Renewal Subscription**"), unless (i) you or GSMA provide written notice of nonrenewal at least 30 days prior to the end of the then-current Subscription; or (ii) your Subscription is otherwise terminated in accordance with this Agreement. GSMA will invoice you for the Renewal Subscription no later than 30 days prior to the expiry of the then- current Subscription.

7.5 In the event of late or non-payment of any invoice for a period of ten days or more following a late payment reminder, GSMA may suspend your Platform account and/or terminate this Agreement in its sole discretion

7.6 The Fees do not include any Tax. To the extent that the Fees are subject to any Tax, the Fees may be increased by the amount of such Tax and GSMA reserves the right to recover such Tax from you at any time. If Tax is required to be paid on the Fees in your own country then you will be liable for its payment, in addition to the amount of the Fees.

7.7 If you fail to pay the Fees by the due date for such payment, then, without limiting GSMA's other rights under this Agreement, GSMA may charge interest on the overdue amount at the rate of two percent above the Sterling Overnight Index Average (SONIA) in effect as of the due date of the relevant payment. Participant shall pay such interest together with the overdue amount.

7.8 GSMA may at any time (i) set off any liability of yours to the GSMA Group against any other liability of yours to the GSMA Group, whether or not either liability arises under this Agreement; and (ii) suspend access to the Fraud Intelligence Service and/or suspend current and future Submissions until such time as all your liabilities to the GSMA Group are paid in full. If the relevant liabilities are expressed in different currencies, GSMA may convert either liability at a market rate of exchange for the purpose of set-off. Any exercise by GSMA of its rights under this clause will not limit or affect any other rights or remedies available to GSMA Group under this Agreement or otherwise.

8. INTELLECTUAL PROPERTY

8.1 You are granted a non-exclusive, non-transferable, non-sublicensable (except to Permitted Affiliates in accordance with clause 12), revocable, royalty-free licence to use, reproduce and modify on an internal basis, the Fraud Intelligence Data you receive via the Fraud Intelligence Service, solely for the Purpose. You will only use such information solely for the Purpose and consistent with the Policies.

8.2 You acknowledge that all rights, title and interest in the GSMA Fraud Intelligence Service, Fraud Intelligence Data, the Platform, and the GSMA Fraud Intelligence Service models, processes, methods, system, data, and all related materials, including all Intellectual Property Rights in any of the above, are retained solely by GSMA and its licensors. You are granted no licence or right, whether express or implied, to use any of the above except as expressly set out in this Agreement.

8.3 You grant to GSMA a non-exclusive, transferable, sublicensable, irrevocable, perpetual, worldwide and royalty-free licence to use Submissions and any other information and data submitted by you to the GSMA Fraud Intelligence Service for the purposes of operating the GSMA Fraud Intelligence Service and related efforts for the Purpose.

8.4 Except as set out in clause 9.5, nothing in this Agreement grants either party any right to use the other party's trade marks without that party's prior written consent. you shall not use the GSMA trade marks or other references to GSMA or the GSMA Fraud Intelligence Service without the GSMA's prior written consent, and in the case of the GSMA's trade marks, subject to a separate licence agreement with the GSMA. Without limiting the foregoing, you will not use any GSMA trade marks or trade names so resembling any trade mark or trade names of the GSMA in a manner likely to cause confusion or deception.

9. CONFIDENTIALITY

9.1 Each party will maintain as confidential at all times, and will not at any time, directly or indirectly (i) disclose or permit to be disclosed to any person, or (ii) use for itself or to the detriment of the other party; any Confidential Information, except:
(a) as required by law or regulation;
(b) as expressly authorised in writing by the other party; or
(c) to the extent reasonably required in relation to, or expressly permitted by, this Agreement.

9.2 For the purposes of this Agreement, “Confidential **Information**” means any information:

(a) relating to the terms of this Agreement;

(b) relating directly or indirectly to the research, development, business plans, marketing, operations, finances of either party; and/or

(c) disclosed by either party to the other party on the express basis that such information is confidential, or which might reasonably be expected by either party to be confidential in nature.

Fraud Intelligence Data received by you via the Fraud Intelligence Service is Confidential Information.

9.3 Information will not be deemed Confidential Information and neither party will have any obligation concerning the use or disclosure of any information which: (a) is or becomes publicly known through no fault of the receiving party; (b) is or becomes known to the receiving party from a third party source other than the disclosing party without duties of confidentiality attached and without breach of any agreement between the disclosing party and such third party; or (c) was independently developed by the receiving party without the benefit of the Confidential Information.

9.4 Nothing in this Agreement will prevent either party from disclosing Confidential Information to the extent it is legally compelled to do so by any governmental or regulatory requirement or any judicial agency pursuant to proceedings over which such agency has jurisdiction; provided however, that prior to any such disclosure, such party must (i) assert the confidential nature of the Confidential Information to the agency; (ii) immediately notify the other party in writing of the agency’s order or request to disclose; and (iii) cooperate fully with the other party in defending against any such disclosure and/or obtaining a protective order narrowing the scope of the compelled disclosure.

9.5 You acknowledge that your organisation name, country, contact information, business description, (e.g. MNO or MVNO) and related information will be incorporated in the Platform and/or associated materials for the purposes of GSMA operating the GSMA Fraud Intelligence Service. You acknowledge that your organisation name and comments (where selected) will be published to Users for the purposes of informing Users of the source and nature of the information in the Submissions.

9.6 You acknowledge that your Submissions and Platform usage information may be provided by GSMA to law enforcement agencies where approved by GSMA. You agree to use reasonable efforts to provide law enforcement agencies with information as reasonably requested by any such agencies in relation to your Submissions and use of the Fraud Intelligence Data.

9.7 Except as expressly provided in this Agreement, neither party will make any press announcements or publicise this Agreement or its contents in any way without the prior written consent of the other party.

10. DATA PROTECTION

10.1 The parties agree that Submissions and other Fraud Intelligence Data containing or relating to unique identifiers (such as IP addresses, telephone numbers/MSISDN) will be treated as Personal Data for the purposes of relevant Data Protection Laws.

10.2 For the purposes of applicable Data Protection Laws, each party:

(a) is an independent Controller of Personal Data;

(b) Processes the Personal Data solely for the Purpose and in furtherance of its legitimate interest in mitigating telecommunications fraud;

(c) will individually determine the purposes and means of its processing of Personal Data, subject to the requirements set out in this Agreement;

(d) will comply with the obligations under applicable Data Protection Laws regarding the processing of Personal Data, which includes taking appropriate security measures to ensure that Personal Data is protected against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage;

(e) will promptly notify the other party in writing of any relevant data breach or if it determines that it can no longer comply with applicable Data Protection Laws or with this Agreement with respect to the Personal Data; and

(f) will provide reasonable assistance as requested from time to time by the other party, and other Users of the Fraud Intelligence Data, by promptly responding to queries as required to assist them in meeting their obligations under any relevant Data Protection Laws including subject access requests or similar queries under applicable Data Protection Laws. The GSMA contact for these requests is FIShelpdesk@gsma.com. Your organisational administrator will be the main point of contact.

10.3 You must inform relevant individuals and/or ensure that your fair processing notice covers the Purpose and the information sharing by you with GSMA and other Users as set out in this Agreement. You must have processes in place to remediate any issues resulting from your decisions in relation to HRN Data.

10.4 Either party may transfer Personal Data from inside the European Economic Area, United Kingdom, and Switzerland to outside those countries if it complies with the applicable provisions on the transfer of Personal Data to third countries in EU Data Protection Laws. The parties agree that the Standard Contractual Clauses will apply with regards to any transfer of Personal Data by the parties from (i) the European Economic Area, United Kingdom, or Switzerland; to (ii) any other jurisdiction. For the purposes of the Standard Contractual Clauses: (1) “data importer” means the party receiving the Personal Data (being GSMA in respect of your Submissions, and you in respect of other Fraud Intelligence Data you receive in relation to this Agreement); (2) “data exporter” means the party disclosing the Personal Data (being you in respect of your Submissions, and GSMA in respect of other Fraud Intelligence Data); (3) for Section II(h), the data importer selects option (iii); and (4) for Section VIII and Annex B, the details of the transfers shall be as specified in the remainder of this Agreement. To the extent of any conflict between the Standard Contractual Clauses and the remainder of this Agreement, the Standard Contractual Clauses will prevail.

10.5 GSMA will keep records of your Submissions and your Platform usage information for a maximum period of seven (7) years, (the **Retention Period**) from the date of the relevant Submission or Platform activity, where upon it will be deleted.

11. YOUR OBLIGATIONS

11.1 You will not represent yourself as an agent of the GSMA for any purpose, nor pledge the GSMA’s credit or give any condition or warranty or make any representation on the GSMA’s behalf or commit the GSMA to any contracts.

11.2 You will not without the GSMA’s prior written consent make any representations, warranties, guarantees or other commitments with respect to the specifications, features, performance, or capabilities of the GSMA Fraud Intelligence Service, the Platform, the Fraud Intelligence Data or related services or otherwise incur any liability on behalf of the GSMA.

11.3 You will ensure that your employees, agents, and contractors, and any other person to whom You share Fraud Intelligence Data in accordance with the terms of this Agreement comply with the terms of this Agreement. You are responsible for the acts and omissions of each of these persons as if they were acts and omissions of yourself.

11.4 You will:

(a) comply with the Policies and GSMA’s reasonable directions in respect of the GSMA Fraud Intelligence Service;

(b) cooperate with GSMA, Users and other Contributors involved in the GSMA Fraud Intelligence Service;

(c) promptly notify GSMA of any breach of your obligations under this Agreement or any other matter which may impact on your ability to perform those obligations; and

(d) not act or omit to act in any way which would or which would reasonably be expected to be considered injurious or detrimental to, to damage or bring into disrepute, GSMA Group, its members or Affiliates, other Users or Contributors, or their brands or reputations.

12. PERMITTED AFFILIATES

You may disclose to the Permitted Affiliates, and authorize the Permitted Affiliates to use the GSMA Fraud Intelligence Services and Fraud Intelligence Data, provided that:

12.1 Permitted Affiliates must comply with the restrictions and obligations upon you under this Agreement. Acts and omissions of Permitted Affiliates are deemed to be acts and omissions by you.

12.2 This Agreement does not create a contractual relationship between the GSMA and any Permitted Affiliates. Permitted Affiliates shall have no right to enforce any term of, or any rights in relation to, this Agreement.

12.3 An entity may only take the benefit of the provisions of this clause 12 for such period as that entity is your Affiliate.

12.4 If you wish to permit further Affiliates to use the GSMA Fraud Intelligence Services or Fraud Intelligence Data, you must obtain the prior written consent of the GSMA in the form of an amended Order Form. Additional fees may apply. For the avoidance of doubt only Permitted Affiliates named on the then current Order Form may use the GSMA Fraud Intelligence Service.

12.5 You or your named Permitted Affiliates may apply to GSMA for login and API credentials for each Permitted Affiliate, in accordance with this Agreement.

13. COMPLIANCE WITH LAWS AND REGULATIONS

13.1 The parties will comply at all times with all applicable laws, rules, regulations, bylaws and standards. Without limiting the foregoing:

(a) the parties will comply with applicable trade sanctions under U.S., United Nations, and any other applicable law, and will not provide access to the Fraud Intelligence Data or the GSMA Fraud Intelligence Service (whether directly or indirectly) to any individual or organization subject to trade sanctions under U.S., United Nations, or any other applicable law; and

(b) each of the parties will comply with all applicable laws, regulations, and codes relating to anti-bribery and anti-corruption including but not limited to the US Foreign Corrupt Practices Act, UK Bribery Act 2010 and will have and maintain in place throughout the Term its own policies and procedures to ensure compliance with such requirements, and will enforce them where appropriate.

13.2 A breach of this clause 12 will be deemed a material breach which is irredeemable for the purposes of clause 14.4.

14. TERM AND TERMINATION

14.1 This Agreement shall be effective from the date that you indicate your acceptance to this Agreement, until terminated or lapsed in accordance with the terms set out in this Agreement (“**Term**”).

14.2 You may terminate this Agreement at any time by 30 days’ written notice to GSMA.

14.3 GSMA may terminate this at any time Agreement by 90 days’ written notice to you.

14.4 Either party may terminate this Agreement with immediate effect by written notice to the other party if an encumbrancer takes possession, or a receiver is appointed, of any of the other party's property or assets; or the other party becomes subject to an administration order or make any voluntary arrangement with its creditors; or the other party goes into liquidation (except for the purposes of amalgamation or reconstruction and in such a manner that the company resulting effectively agrees to be bound by or assume the other party's obligations under this Agreement); or if the other party ceases, or threatens to cease, to carry on business; or if the other party suffers any similar process under the law of the other party's domicile or place of jurisdiction.

14.5 GSMA may terminate this Agreement with immediate effect by written notice to you:

(a) if you commit a material breach of your obligations under this Agreement which is incapable of remedy or which remains uncorrected for a period of seven days after receiving written notice from GSMA of the breach; or

(b) in the event of any relevant legislative or regulatory change which in the opinion of GSMA, acting reasonably, requires this Agreement be terminated or suspended.

14.6 GSMA reserves the right at its sole discretion to deny access to the service or suspend access (offering a pro-rata refund) to the service to entities who, after reasonable investigation by GSMA, using evidence from a variety of sources including operators subject to fraud perpetrated by the entity, determines that the entity is using the service to support fraudulent activity. You accept that, in the event of any actual or reasonably suspected breach of this Agreement by you, including any misuse of the Platform or Fraud Intelligence Data, and without limiting the rights and remedies of GSMA under this Agreement or otherwise at law, GSMA may, at its sole discretion:

(a) terminate or suspend this Agreement, and discontinue your access to the Platform without notice; and/or

(b) communicate the actual or alleged breach or infringement to Users of the Platform, particularly Users of your Submissions; or

(c) withdraw or suspend all or some of your Submissions from the Platform;

with no liability to GSMA.

14.7 Upon termination or expiry of this Agreement for any reason, no refunds, discount or credit will be offered in respect of the termination, expiry, or failure by you to renew your Subscription, except where:

(a) GSMA terminates this Agreement for convenience pursuant to clause 14.3; or

(b) you terminate this Agreement pursuant to clause 18,

while you currently hold a Subscription, in which case GSMA will provide a pro rata refund for the remaining months prepaid in your Subscription.

14.8 Upon termination or expiry of this Agreement for any reason whatsoever:

(a) your access to the Platform will be withdrawn;

(b) GSMA will retain your Submissions for use within the High Risk Numbers Service and GSMA Fraud Intelligence Service for the remainder of the Retention Period;

(c) your licence under clause 8.1 for any Fraud Intelligence Data that you received prior to the effective date of termination shall continue, subject to the requirements set out in this Agreement;

(d) you may continue to modify your existing Submissions in accordance with clause 5.1, by contacting GSMA at FIShelpdesk@gsma.com;

(e) termination will be without prejudice to either party's rights and remedies in respect of any breach of this Agreement by the other party, where the breach occurred before the termination of this Agreement; and

(f) the provisions of clauses 3.2, 4.4(e), 5.3, 7.8, 8, 9, 10, 11, 14.7, 14.8, 15, 16, 17 and 19 of this Agreement, together with such other provisions reasonably required to give effect to those clauses or which by their nature are intended to survive termination, will remain in full force and effect following termination or expiry.

15. DISCLAIMERS AND BASIS OF SERVICE PROVISION

GSMA and Users provide and use the GSMA Fraud Intelligence Service and Fraud Intelligence Data in good faith for the benefit of the wider telecommunications ecosystem. Accordingly**:**

15.1 You accept that GSMA, by providing you with access to the Platform, is providing an exchange platform for information provided by numerous third party data sources. GSMA does not perform any checks or vetting, and does not accept any responsibility for the accuracy or completeness of the Fraud Intelligence Data. You acknowledge and agree that GSMA Group and its contributors and licensors have no responsibility for the accuracy, currency or completeness of Fraud Intelligence Data obtained via the Platform or otherwise**.**

15.2 The Platform, Fraud Intelligence Data, and any other related information or services provided by (i) GSMA or any of its affiliates, and/or (ii) Contributors; are provided “as is” and without any warranty of any kind. Users access the Platform without warranty or representation of any kind, and will not be liable for any failure or delay to implement Fraud Intelligence Data.

15.3 For the avoidance of doubt, GSMA and other Users accept no responsibility for third party claims based on or in relation to their respective use of Fraud Intelligence Data or otherwise in relation to the Platform, including without limitation claims by device owners or subscribers in relation to network performance. you indemnify and hold harmless GSMA and other Users against all costs, losses and expenses arising from or in relation to any such third party claims.

15.4 All warranties, whether express, implied, or statutory, including without limitation any implied or other warranties of merchantability, fitness for a particular purpose, quality, accuracy, completeness, timing, or title are expressly disclaimed and excluded by GSMA, you, and other Users.

16. LIABILITY

16.1 Notwithstanding any other provision of this Agreement, nothing in this Agreement excludes or limits any person’s liability for: (i) any death or personal injury caused by its negligence; (ii) any fraud or fraudulent misrepresentation; or (iii) any other liability which cannot be excluded under applicable law.

16.2 Subject to clause 16.1, no person (whether you, GSMA, any other User, or otherwise) will be liable in relation to the Fraud Intelligence Service for any loss of profits, loss to reputation, loss of contracts, or any indirect, punitive, special or consequential loss or damage.

16.3 Subject to clause 16.1, each party’s total aggregate liability to each other under or in relation to the GSMA Fraud Intelligence Services will not exceed USD $1,000 (one thousand US dollars).

16.4 GSMA operates the Platform and the GSMA Fraud Intelligence Service for the benefit of the global mobile ecosystem, for the purposes of combatting mobile device crime and fraud. you acknowledges that this clause 16 represents a reasonable allocation of risk and that, in the absence of these provisions, the terms of this Agreement would be substantially different.

16.5 This clause 16 shall not apply to limit fees payable pursuant to clauses **Error! Reference source not found.** and 7.7.

17. NOTICES

17.1 All notices, requests, consents, claims, demands, waivers and other communications in relation to this Agreement must be in writing and addressed to the parties at the following addresses:

(a) If to GSMA: *GSMA Ltd., Attn: Deputy General Counsel, 165 Ottley Drive, Suite 150, Atlanta,* *Georgia 30324, United States of America*; with an advance copy to FIShelpdesk@gsma.com and legalnotices@gsma.com.

(b) If to you: To the email address in your account details, as updated by you from time to time via FIShelpdesk@gsma.com or via your account settings at www.gsma.com/services.

17.2 Any notice required to be given pursuant to this Agreement will be deemed to be properly given immediately upon delivery.

18. MODIFICATIONS AND PREVIOUS VERSIONS OF THIS AGREEMENT

18.1 This Agreement supersedes any earlier agreements between GSMA and you regarding your use of the GSMA Fraud Intelligence Service or submissions to GSMA of information falling within the categories set out in Schedule 2 (including under any other previous service or programme names, such as the High Risk Ranges List sent from the GSMA Fraud and Security Group (FASG)).

18.2 GSMA may amend this Agreement by not less than ninety (90) days' written notice. Your continued use of the GSMA Fraud Intelligence Service and/or Platform following notice of the changes will be deemed to constitute acceptance of the amended terms and conditions. In the event that you do not wish to accept the amended Agreement, you may terminate this Agreement on written notice to GSMA not less than ten (10) days prior to the effective date of the relevant amendment, in which case you will receive a pro rata refund in accordance with clause 14.7.

19. GENERAL

19.1 This Agreement is the complete, final and exclusive entire agreement between the parties relating to the subject matter and supersedes any and all prior agreements, representations, communications, undertakings, or discussions relating to the subject matter hereof.

19.2 If any term, provision, covenant or condition of this Agreement is held invalid or unenforceable for any reason, the parties agree that such invalidity shall not affect the validity of the remaining provisions of this Agreement and further agree to substitute for such invalid or unenforceable provision a valid and enforceable provision of similar intent and economic effect.

19.3 You may not transfer or assign any of your liabilities or rights under this Agreement to any other person without the prior written consent of GSMA, such consent not to be unreasonably withheld. GSMA may at any time subcontract, transfer or assign any of its liabilities or rights under this Agreement to any other entity upon written notice to you.

19.4 No failure or delay by either party in enforcing its respective rights will prejudice or restrict the rights of that party, and no waiver of any such rights or of any breach of any contractual terms will be deemed to be a waiver of any other right or of any later breach. The rights powers and remedies provided in this Agreement are cumulative and are in addition to any rights, powers or remedies provided by law.

19.5 No person shall be liable for any failure to perform or delay in performance of any of its obligations under or in relation to this Agreement caused by circumstances beyond the reasonable control of that person (which may include but not be limited to one or more of the following: governmental regulations; riot; civil unrest; military action; terrorism; earthquake; disease or epidemic; storm; flood; inability to obtain supplies of power, fuel, or transport; exercise of emergency powers by any governmental authority) (a "**Force Majeure Event**"). A party claiming to be affected by a Force Majeure Event will not be entitled to invoke the provisions of this clause to the extent that such party fails to take all reasonable steps to prevent, avoid, overcome and mitigate the effects of such Force Majeure Event.

19.6 Nothing in this Agreement is intended to create a partnership or joint venture of any kind between the parties, or to authorise any party to act as agent for the other.

19.7 Except as expressly stated otherwise in this Agreement, each party shall bear full and sole responsibility for its own expenses, liabilities and costs of operation.

19.8 Subject to clause 18, this Agreement may not be varied, modified, altered, or amended except by agreement in writing by the parties' duly authorised representatives.

19.9 Save for the provisions of clause 15, which may be enforced by and between Users, no person who is not a party to this Agreement shall have any right under the Contracts (Rights of Third Parties) Act 1999 (UK) or otherwise to enforce any term of this Agreement.

19.10 This Agreement shall be construed and interpreted in accordance with the laws of England excluding its rules for choice of law and the parties hereby submit to the exclusive jurisdiction of the English Courts located in London.

19.11 This Agreement was written in English. To the extent any translated version of this Agreement conflicts with the English version, the English version controls.

SCHEDULE 1
SERVICE DESCRIPTION

General

Subject to the terms of this Agreement, users may use the Fraud Intelligence Service (FIS) to:

- submit and consume HRN Data which has been linked to fraudulent activity;
- analyse fraud information associated with Fraud Intelligence Data;
- analyse traffic sources and destinations against operator information;
- analyse anomalies identified by the Platform; and
- access the Fraud Intelligence Data via your local fraud management system using the FIS API.

Accessing the Fraud Intelligence Service

The FIS Platform web-based user interface and FIS API are available 24 hours per day, (365 days a year. Access to the FIS is achieved at the GSMA's Fraud and Security services pages at www.gsma.com/services. User is entitled to be issued up to ten sets of login credentials, or other amount as defined in your Order Form, for its organisation to access the FIS. Access to the API may be arranged by contacting FraudIntelligence@gsma.com. You are entitled to one API access point(s) unless stated otherwise in your Order Form. You are entitled to the quantity of API calls per (Subscription) year as defined in your Order Form.

A summary of FIS functionality is described, as follows, in this Schedule 1. A summary of the data held in, or accessible from, the Platform is described in Schedule 2.

HRN Data Submissions

User may submit HRN Data records comprising of:

- A number or range
- A mandatory associated Fraud Label (for more information see Schedule 2);
- Optional Status ("active" meaning less than 18 months old or "obsolete" meaning more than 18 months old)
- An optional accompanying comment (for more information see Schedule 2).

Submissions may be made manually via the Platform web based user interface or as a list in the form of an Excel file as described in the User Guide. The Platform assigns the Contributor's organisation identity to each record. The Platform performs basic error checking on Submissions, e.g. if a fraud label is not supplied with an HRN Data record, and informs the User accordingly. User may edit/delete submitted HRN Data records via the web based user interface. HRN Data is sourced from operators or representative associations, pooled together for use by the User community and changes are continuously updated and refreshed.

Exporting HRN Data

User may export for download all, or a subset, of the HRN Data submitted to the Platform, and checked by the Platform, in the form of an Excel or CSV file at a frequency of:

- once a month; and
- a further time within the 24 hours following each HRN Data Submission by you.

The export file contains a list of selected HRN Data records each containing where populated:

- A telephone number or range;
- The associated Fraud Label;
- The accompanying comment;
- The organisation who submitted the record;
- Status indicating an active or obsolete record;
- Date of Submission and last edit; and
- Issues or anomaly flags.

Data Validity and Storage

- When a HRN Data record has been stored for 18 months the Platform marks the record as obsolete.
- HRN Data is stored in the Platform and available for use for up to seven years.

Data Correlation and Anomaly Detection
The Platform systematically compares HRN Data, IR.21 Data and other telecoms data sources (RAEX, ipData.co, OSINT) with each other when new submission or changes are made by Users. The Platform flags anomalies worthy of investigation to the User via the Analysis Tools below. Such items are given an issue label describing an anomaly. Examples of anomalies include:

- Identification of an HRN Data record associated with an operator
- IP address associated with a location which is not where the IP address is registered
- Duplicate or overlapping number ranges or IP addresses
- Active numbers falling outside operational number ranges

Data Correlation and Anomaly Detection results may be exported and downloaded.

Dashboards
User may select and configure a series of dashboards including:

- World HRN threat map
- World IP address anomaly heatmap
- Ratio of HRN Data relating to mobile vs non-mobile sources

Settings
User may define private labels for use in filtering data according to internal conventions. User may show or hide alerts and notifications.

Analysis Tools
User may use a series of analysis tools provided via the web based user interface. Data definitions are given in Schedule 2.

HRN Analysis
User may view all, or filtered, lists of HRN Data records including the HRN numbers, date or submission, source of submission, fraud label, status, country location and operator of HRN Data, issues, sightings, connections and comments.
User may filter HRN Data by date of submission, number range, fraud label, issue, connection, country, operator in order to analyse fraud from different perspectives. Each filtered list may be downloaded.
User may access details of an HRN Data record and find contact information for the Contributor, add a sighting, add public or private labels and add public or private comments.

Mobile Number Range Analysis
User may view all, or filtered, lists of E.164 number data associated with Mobile Operators including number ranges, operator name, TADIG code, country location, technology of connection, any HRN Data associated with those ranges and any associated issue flags with the data. User may use this data to research any suspected fraud identified on its network. Number data may be filtered by date of update, country code, network destination code, start and end range, operator identity, connection type, number range description or issue.

MCC/MNC Analysis
User may view all, or filtered, lists of E.212 and E.214 number data associated with Mobile Operators including operator name, TADIG code, country location, technology of connection, any HRN Data associated with those ranges and any associated issue flags with the data. User may use this data to research any suspected fraud identified on its network. Number data may be filtered by date of update, country code, mobile network code, operator identity, or connection type.

Operator IP Range Analysis
User may view all, or filtered, lists of IP address information associated with Mobile Operators including IP address, IP address type, operator name, TADIG code, country location, and any associated issue flags with the data. User may use this data to research any suspected fraud identified on its network. Number data may be filtered by date of update, country location, IP city, IP country, ASN, IP address type, operator identity, connection type, label or issue.

API

The Platform provides an API for accessing the FIS Data. The API is based on secure RESTful/JASON technology and is specified in the GSMA Fraud Intelligence Service API Specification. Your back office or fraud management system may initiate API calls and receive results. API calls may request data about:

- High Risk Numbers
- Mobile Number Ranges
- MCC/MNC
- Operator IP Ranges

API call may request results comprising of:

- Metadata: get status values, labels or fraud types
- All: get similar items, e.g. HRN numbers, IP addresses
- FindBy: get information for a specific item e.g. a HRN number or IP address

Fraud Intelligence Service Availability and Support

GSMA will use commercially reasonable efforts to provide the Fraud Intelligence Service with target availability in excess of ninety-nine point nine-five percent (99.95%) per annum in respect of the GSMA's controlled Platform infrastructure. Data is backed up on a regular basis for disaster recovery purposes. User may use the help desk for general support concerning operation of the system and data content between 08:30 and 17:00 CET (or CEST when applicable), from Monday to Friday on Business days, using FIShelpdesk@gsma.com. Business days are defined as days where banks in Luxembourg are open for business. Faults may be reported to the help desk twenty-four by seven (24x7) and will be resolved as quickly as possible. User is responsible for User's connectivity to the Fraud Intelligence Service. Customer will gain access to user guide documentation on successful registration to the service.

SCHEDULE 2
CATEGORIES OF FRAUD INTELLIGENCE DATA

A. High Risk Number Data (HRN Data)

- HRN Data records, including HRN numbers
- Dates of HRN Submissions
- Contributor submitting HRN Data
- Sightings, the number of times fraud has been attributed to an HRN number.
- Fraud Labels appended to an HRN Data record by the Contributor (as described below).
- Comments appended to an HRN Data record by the Contributor (as described below).

B. Other Fraud Intelligence Service Data

Comments (Public and Private)	Users can make free form comments on HRN Data and make them visible to all Users or just Users within their own organisation
Connections	The technologies associated with numbers in the database, i.e. 2G to 5G and other features such as CAMEL
Dates	Dates of operator information updates
E.164	E.164 mobile telephone number ranges identifying the E.164 numbering resources available to an operator
E.212 and E.214 number ranges	E.212 and E.214 number ranges identifying the E.212 and E214 numbering resources available to an operator
Fraud Labels	System-defined labels describing a particular type of fraud. Note: related descriptions of fraud can be found in the GSMA FF.21 Fraud Manual.
Groups	Information sharing groups
IP address country location	The country location of an IP address as reported by an external registry
IP Address Type	IP Address type, for example APN, M2M, DNS, etc.
Issues	Flags describing errors or anomalies identified by the Platform
Labels (Global and Private)	Users define and assign their own fraud labels to HRN Data and make them visible to all Users or just Users within their own organisation
Mobile Operator IP Ranges	Mobile Operator IP Ranges identifying a variety of network gateways and Access Point Names (APNs)
Notifications	Messages/alerts generated by the system for the User
Number range description	MSISDN number ranges, Global title number ranges, MSRN number ranges, Number portability, Network nodes, Hosted networks
Read status	Whether user has processed an HRN number record
Roaming partners	Operators with which the User has an active roaming agreement.
Sightings	The number of times fraud has been attributed to an HRN number
Status	Whether HRN data is “active” meaning less than 18 months old or “obsolete” meaning more than 18 months old
TADIG Codes	Alpha/numeric identities of operators
Tags	Types of number, e.g. premium rate
User contacts	User-assigned contacts for handling fraud enquiries