**i3Forum Fraud Data Sharing Guidelines:**

The i3Forum Fraud Workgroup may be involved in the discussion and sharing of fraud risk information which may be used by the industry in the detection and prevention of potentially fraudulent call routing activity (“**Fraud Data**”). Since the Fraud Data involves the potential sharing of information by competitors, it is important that we establish guidelines to ensure the use of the Fraud Data is closely aligned with data protection and competition law requirements. The following principles and guidance describe the controls which are required to be in place to protect the exchange of Fraud Data, and to ensure that the highest possible level of fairness and transparency are observed:

**Guidelines of Use of the i3Forum Fraud Data**:

1. **Purpose:** The intended purpose for the use of the Fraud Data must only be used for the explicit and legitimate purposes of identifying and mitigating fraudulent activity in the industry and to enable quicker action in cases of similar fraud and each member of the group agrees that the Fraud Data shall not be further processed in a way incompatible with those purposes.
2. **Reciprocity:** The Fraud Data relies on member data. Members are encouraged to contribute their own cases to receive benefit from the data shared by other members.
3. **Sharing of Non-Commercially Sensitive Information**: The information shared in the Fraud Data must be non-commercially sensitive information and shall not contain pricing or commercially confidential information.
4. **EU GDPR Compliance**: The GDPR specifically recognizes the importance of fraud prevention and any processing of personal data contained in the Fraud Data must be in compliance with Recital 47 which states “The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned…” (See <https://www.privacy-regulation.eu/en/recital-47-GDPR.htm> )
5. **Format of Sharing:** The format of the Fraud Data share will be limited to emails directly addressed to the group members and including the use of group mailbox. The identity of the sender should be made clear and the date of the incident should be mentioned when reporting Fraud Data. All emails must be marked as Confidential and the workgroup shall agree on a subject format for the emails so that the information shared is consistent and easily recognizable.
6. **Anonymization of Supplier/Operator:** Supplier/Operator subjects must not be identified in the Fraud Data (except where such information is available in the public domain) and the data exchanged shall be limited to the call number (A or B number) and routing type only (eg: Direct or Direct + 1). For clarity, a Supplier/Operator which directly terminates the traffic may only be identified where such information is publicly available (eg: where the Supplier/Operator is publicly identified as the number range owner), however, indirect suppliers should not be identified as this may be deemed as commercially sensitive information)
7. **Fraud Classifications:** Potential fraud call number must be associated by the applicable fraud classification as determined by the Fraud Workgroup.
8. **Restrictions on Use of the Fraud Data:** The Fraud Data reported by a carrier within the group, will not be used for fraud disputes, will not be used as evidence of fraud by the originating carrier (in case the latter is also a member of the working group). Further, the Fraud Data reported cannot be used for police/regulatory reports. The Fraud Data sharing and Fraud disputes management must be kept as separate processes and one should not influence the other. The Fraud Data reported by a carrier within the group will always be subject to Accuracy and Accountability requirements as set forth below.
9. **Independent Action:** Actions for fraud detection and prevention should be taken individually by a member and should always be done after exercising independent judgment. All members must always unilaterally decide to use the information contained in the Fraud Data according to your company’s risk appetite.
10. **No Restraint of Trade/Boycotting/Blacklisting:** It is critical to avoid concerted activity and discussions on boycotts or blacklisting that unreasonably restrain trade. Keep in mind, this includes even informal discussions among companies concerning positions on boycotting or blacklisting. A group boycott or blacklist is an agreement between competitors to refuse to conduct business with another competitor, individual, company, or consumer to restrain competition.
11. **Transparency:** If queried, supplier/operator subjects have a right to know how Fraud Data related to them was determined and shall have an opportunity to correct any inaccurate data.
12. **Lawfulness (Standard of Proof):** Cases filed to the Fraud Data must be supported by evidence and meet the following standard of proof:
    1. That there are reasonable grounds to believe that a Fraud or Financial Crime has been committed or attempted;
    2. That the internal supporting evidence standard for reporting Fraud must be clear, relevant and rigorous such that the member could confidently report the conduct to the Fraud Workgroup; (Note: A clear standard to consider is whether the reporting party could confidently report the conduct to law enforcement); and
    3. In order to report Fraud Data the member must have either: (i) initiated internal fraud investigations; (ii) rejected, disputed, blocked, withdrawn or terminated a Product/service on the basis of the alleged fraud; or (iii) reported the fraudulent activity to law enforcement.
13. **Fairness (Proportionality):** Members must independently determine to interpret their response to the Fraud Data in a proportional manner according to their own risk appetite and the product being assessed.
14. **Accuracy:** All data that is captured must meet the Standard of Proof and be accurate as of the date of exchange and should the disclosing carrier notice a change after disclosure, then the Fraud Data must be updated to ensure accuracy. The Members acknowledge any Fraud Data provided may change over time and become ‘non-fraudulent’ after a period of time and any Member relying on the Fraud Data should independently check as to whether the number(s) remains fraudulent or not.
15. **Confidentiality:** All information (including Fraud Data) shared within the group shall be treated as confidential and shall only be used for the Purpose of Sharing as set forth above (“Confidential Information”). The receiving party shall keep the Confidential Information received from any disclosing party confidential and shall not disclose or disseminate the Confidential Information outside of the group members (except where a receiving party becomes compelled by an order of any court of competent jurisdiction or by law).
16. **Accountability:** The member reporting Fraud Data will remain responsible for following the i3 forum fraud dispute resolution recommended processes and or other bilateral contractual clauses, outside the Fraud Data sharing arrangement set forth herein, even if as supplier or recipient of service involved is another i3Forum member.