1.0 Purpose

The purpose of this instance of the Telecom Data Trust Framework (TDTF or Trust Framework) is to specify a trusted framework between telecom-centric identity providers and parties certified under this TDTF to use telecom sourced identity data for verification services. This Trust Framework will provide general guidelines for the content to be exchanged, and describe the process by which these trusted relationships may be independently audited.

2.0 Definitions

- **ID Provider or IDP** – An entity with access to authoritative identity information and/or attributes.
- **Relying Party or RP** – An entity requiring telco-based identity information either for its own internal purposes (in which case the entity is a “direct relying party”) or for the purpose of providing a service to other entities (in which case the entity is a “reselling relying party”).
- **Certified Transaction** – A transaction certified by this Trust Framework.
- **Identity Subject** – The person whose identity information is verified by an ID Provider.
- **Auditing Party** – An entity tasked with verifying the level of compliance of an ID Provider or Relying Party to the rules and standards of this Trust Framework.
- **Verification** – The act of providing confirmation that the information supplied is true. Under this Trust Framework, an ID Provider provides verification to a Relying Party by confirming the extent to which the identity attributes passed by the Relying Party to the ID Provider are true.
- **Data Caching** – The act of storing authoritative identity information and/or attributes provided by an IDP and then re-using that authoritative identity information and/or attributes in place of making a new request.
- **Telecommunication Service Provider (TSP)** – A provider of telecom services as defined by the FCC in CFR 64.1201(a)(2).
- **BNA** – means Billing Name and Address and is the name and address provided by the customer to a TSP as the authoritative record used by the TSP to direct bill for its services.
- **BKNA** – means Best Known Name and Address and is a name and address record that is not directly acquired through a TSP but through a third party. BKNA is not considered authoritative data under this Trust Framework.
- **CPNI** – Means Customer Proprietary Network Information and is any information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a TSP, and is made available to the carrier by the customer solely by virtue of the TSP/customer relationship; including information contained in bills pertaining to the telephone exchange service to telephone toll service received by a TSP; except that such term does not include subscriber list information.
- **Acceptable Use Applications**:
o Fraud Prevention
o ID Verification
o Law Enforcement
- **Per Query Basis** - Means that each Query shall be initiated in connection with a specific transaction between Customer and an end user when such end user engages in a transaction with Customer.
- **OIX Telecom Data Trust Framework Working Group** ("Working Group") – Signors of the original OIX Telecom Data Trust Framework Working Group or subsequent members approved by the original Working Group members.
- **OIX Board** – The Board of Directors and Executive Committee of the Open Identity Exchange.

### 3.0 Content

As a trust framework specifically designed for verifying known information, any personally identifiable information (PII) will be one directional from the Relying Party to the ID Provider. The ID Provider will provide no PII to a Relying Party as part of a Verification transaction. The PII required by the ID Provider for Verification can vary by implementation and ID Provider, but is always information provided by the end user of the TSP and is presumed to include a full 10-digit phone number, the name of the subscriber on the account and the physical address to which the subscriber’s bill is sent. The ID Provider who services these Verification requests will provide confirmation back to the Relying Party as to the correctness of either the asserted name or address, or both. Subject to acceptable use policies, the ID Provider may also provide back additional meta-data to the Relying Party such as an approximate time for which the account has been active. No meta-data content will be provided that the ID Provider deems in violation of CPNI regulations.

### 4.0 Data Retention, Financial Obligations & Acceptable Use

This Trust Framework provides for no disclosure of regulated content by an ID Provider. However, for data to be verified, content must be passed from a Relying Party to an ID Provider. This content will be used solely for the purpose of verifying the information provided. The name and address content being received by the ID Provider from the Relying Party will not be provided to any other party by the IDP, nor will it be retained or used for any purpose other than what is required to process and administer the transaction.

Likewise, this Trust Framework constrains all Relying Parties from Caching or retaining Verification results for later use. A single Verification query and result are intended only to provide information for a single, transient transaction occurring in real-time. A record of a Verification transaction may, however, be retained by a Reselling Relying Party for the purpose of calculating charges for their customers or reconciling payments to ID Providers. Information retained for these purposes is limited to the transaction date, the Verification response, the requesting Relying Party, the ID Provider who provided the response, and the input parameters supplied in the Verification query. Direct Relying Parties (those not reselling a Verification result) may maintain a record of the Verification transaction for the purpose of providing an audit trail. No meta-data, as defined in Section 3.0, above, may be retained.
in logging or accounting records. Under no circumstances may any part of a Verification transaction be subsequently used by a Relying Party or a Relying Party’s customer for the purpose of reducing or avoiding transactional charges owed to an ID Provider.

ID Providers must contractually restrict the use of the results of any ID Provider certified response, whether or not it contains any personally identifiable data, only for purposes specifically allowed in this section. Additionally, transactions allowed under this Trust Framework, must be limited to in-process transactions, whether the transaction was initiated in-person, over the phone or on-line and cannot be used for marketing, to update or correct any third party database, or for demographic assessment purposes unless otherwise agreed to in writing by the ID Provider.

Acceptable uses under this Trust Framework include Fraud Prevention, Identity Verification and Law Enforcement. Certification under this Trust Framework requires all Relying Parties to contractually prevent access to a Verification result for any uses other than the aforementioned, including, but not limited to uses that assist in or promote commercial marketing.

**5.0 Audit Process and Requirements**

The three primary goals of this trust framework are:

1. To define what information transfer or exchange is allowable;
2. To certify that a Relying Party adheres to the requirements under this Trust Framework regarding the retention of Verification results, financial obligation and acceptable use; and
3. To certify that an Identity Provider adheres to the requirements under this trust framework when it provides or verifies asserted identity attributes and that assertions of a particular Level of Assurance meet the definitions and guidelines for such Levels of Assurance as stated below.

The audit process below outlines the required affirmations that must be certified by an authorized TDTF Auditing Party. The following assumes that identity attributes are asserted by a Relying Party and verified (or not) by an Identity Provider.

**Level of Assurance** – The LOA is the declaration the ID Provider makes to the Relying Party that they have contractual permission to provide the requested data to the Relying Party and that the quality of the data being used as the source for verifying the asserted identity attributes meets the definition of an asserted Level of Assurance as defined and documented below. Documentation of the ID Provider’s contractual permission includes proof that the underlying owner of such data (the TSP) has given approval of its use, and that a contract exists between the TSP and the ID Provider if those two entities are not the same entity. The ID Provider’s asserted Level of Assurance may be defined in one of two ways: 1) contractually, where all identity Verifications provided under a contract have the same level of assurance; or, 2) transactionally, where a Level of Assurance is provided by the ID Provider as part of the response to each identity Verification transaction. Contractual LOA must be the same for all
transactions that fall under a specific contract. Transactional LOA can vary from one transaction to another within a specific contract. Audit Procedures must verify that the qualifications for a given Level of Assurance of either the whole contract (for Contractual LOA) or of all transactions having the same LOA within a contract (for Transactional LOA) meet the definitions and requirements for the asserted Level of Assurance. Audit Procedures must verify that a Verification transaction labeled as a particular LOA is not substituted for, or provided in lieu of, a Verification transaction of a higher LOA. For example, some IDPs can be said to be certified under this Trust Framework for up to Level 2 Assurance but other IDPs may only be certified for up to Level 1 Assurance.

Following are the Levels of Assurance that may be declared by an ID Provider under this Trust Framework and passed on to Relying Parties. Audit procedures must verify that Verification transactions sold as a particular LOA meet the corresponding rules, guidelines and definition for the appropriate asserted Level of Assurance:

- **Level 1** – An LOA of 1 (the lowest level) is appropriate when 1) an ID Provider can verify an Identity Subject’s information but does not have a contractual relationship with the owning TSP or otherwise lacks contractual permission to use its data for Verification or to provide Verification services on such TSPs behalf (ID Provider sources the Identity Subject’s information through a 3rd party source); or 2) the source against which an identity subject’s information will be compared for the purpose of Verification is not controlled or protected in such a way that an identity subject’s information cannot be modified without an authoritative, third-party verification. An example of a LOA 1 is the Verification of an Identity Subject’s information with data aggregated from sources other than the TSP such as Best Known Name and Address (BKNA) data or data over which the consumer has control or the ability to modify such as CNAM or non-authoritative carrier data such as Directory Assistance.

- **Level 2** – An LOA of 2 is appropriate when 1) an ID Provider can verify an Identity Subject’s information using TSP data and has a contractual relationship with the owning TSP or has contractual permission to use its data for Verification or to provide Verification services on its behalf; and, 2) the source against which an Identity Subject’s information will be compared for the purpose of Verification is controlled or protected in such a way that an Identity Subject’s information cannot be modified without an authoritative, third-party verification. An example of a LOA 2 is the Verification of an Identity Subject’s information with data sourced directly from the TSP such as Billing Name and Address, or BNA.

- **Level 3** – An LOA of 3 under this Trust Framework is appropriate when the underlying data used for Verification is compliant with LOA2, AND the identity of the subject is further verified through an additional factor of authentication such as via a pass code delivered to the Identity Subject’s mobile phone or physical address. An example of Level 3 is the Verification of an Identity Subject’s information using BNA and additionally using an Out-of-Band method, such as an SMS verification, to confirm the user who is asserting that identity has actual control over the device to which that BNA information is associated.

**Levels of Protection** – The LOP is the assurance a Relying Party gives to an ID Provider as to the protections and use restrictions to which the Relying Party will adhere and which it will allow to be
verified by independent auditors. A Relying Party verified by an external, independent auditor to achieve at least a Level 2 LOP can be noted as being a Certified Relying Party under this Trust Framework.

- Level 1 – There is no Level 1 LOP applicable to this Trust Framework.
- Level 2 – An LOP of 2 is the minimum LOP required in the Trust Framework and is appropriate when a Relying Party is found, by an independent auditor, to adhere to a reasonable standard of security and safety in order to prevent a breach. It must also adhere to all audit requirements for accessing and handling an Identity Subject’s information. Furthermore, a Relying Party must comply with these requirements for Content Management and Acceptable Use:
  - Relying Party will not cache or store responses from an ID Provider per Section 4 of this Trust Framework
  - Relying Party will not use the results of a Verification query for marketing, demographic assessment, or to update and/or correct any third party databases. RP must use responses on a per transaction basis strictly for one of the following three purposes:
    1. identity verification
    2. fraud prevention
    3. law enforcement.

Certifications for ID Providers and Relying Parties by an Independent Auditor must be renewed no less than every thirty six (36) months at the expense of the party being audited. Additional audits may be requested by a simple majority vote of the voting members of the Telecom Data Working Group if evidence is brought to the Working Group that suggests an ID Provider or Relying Parties is no longer adhering to the terms of this Trust Framework. Such additional audits will be paid for by the audited party unless such party is found to be in compliance with the terms of the Trust Framework. The audited party may opt-out of the Trust Framework by written notification to the OIX Board and the Working Group and by ceasing to market and advertise their certification. If the audited party does not opt-out of the Trust Framework and a subsequent audit fails, the party will have 120 days to correct the failure and be re-audited for compliance. If, after 3 months, an approved auditor is not able to verify compliance, the ID Provider or Relying Party’s certification will be revoked. At such time the Open Identity Exchange may, on its own authority and schedule, remove the affected ID Provider or Relying Party from its list of certified providers of services documented within this Trust Framework.

### 6.0 Certification

Following are the requirements for certification under this Trust Framework:

- **ID Providers**
  - Subject to audits that demonstrate security processes in place to protect the identity assertions provided by Relying Parties to the ID Provider, per Section 4, above.
  - Demonstrate that all Verification results or attributes labeled as having a particular LOA meet the rules and guidelines for that LOA as stated in Section 5, above.
Identify the Level of Assurance (and have such verified by the independent auditor) for each Verification result if requesting certification for a Transactional Level of Assurance. Identify the Level of Assurance (and have such verified by the Independent auditor) of all transactions under a contract if requesting certification for a Contractual Level of Assurance.

Demonstrate that all requirements for an ID Provider are met as documented in sections 3, 4, 5 and 8 of this Trust Framework.

- **Relying Parties**
  - Demonstrate that Verification results are not cached
  - Demonstrate that all Verification requests are performed on a Per Query Basis.
  - Demonstrate that the Level of Assurance of a Verification result is no higher than the Level of Assurance acquired from an Identity Provider in cases where the Relying Party is reselling Verification results to other parties.
  - Demonstrate that consent was obtained from the Identity Subject to permit verification through an ID Provider or from a law enforcement or governmental agency that has been authorized by law, subpoena or court order to request verification of an account without the Identity Subject’s consent
  - Demonstrate that the Level of Protection afforded verification results received as part of a Certified Transaction meet the minimum allowable Level of Protection as documented in Section 5, above.
  - Demonstrate that all requirements for a Relying Party are met as documented in sections 3, 4, 5 and 9 of this Trust Framework.

- **Auditing Organizations**
  - Be independent of the entity being audited
  - Be approved by a simple majority of the voting members of the OIX Telecom Data Trust Framework Working Group as an organization deemed to have sufficient telecommunications industry expertise to be able to knowledgeably audit compliance with this Trust Framework
  - Meets the guidelines or other requirements as being certified under one or more of the following standards or such standard as the OIX Board deems a reasonable minimum standard:
    - IRCA 802
    - ISO 17021
    - ISO 27006

An entity may apply for certification as either an ID Provider, a Relying Party or both by submitting a report from a Trust Framework Auditor certifying their compliance with the terms and requirements of the Trust Framework. Such submissions may be made to either the Chairperson(s) of the Telecom Data Trust Foundation Working Group or to the Executive Director of the Open Identity Exchange.
7.0 ID Provider Additional Responsibilities

Additional responsibilities of an ID Provider who is certified under this Trust Framework include the following.

Verification Service Provision – Provide the verification service via a known standard, such as XML over HTTP or HTTPS or SS7 (either directly or through an agent).

OCN List – The ID Provider must be able to provide a list of TSP entities for which the ID Provider can provide Verification. Ideally, this list should be a standard set of ASEC/AO/OCN values within the NANPA controlled geographic area or an equivalent standard in other jurisdictions. Such a list can be made available to Relying Parties either transactionally, where an OCN is passed by the Relying Party to the ID Provider who returns an indication of whether or not Verifications can be performed for this entity, or alternatively (and preferably) as a list of TSP entities for which Verification services can be provided. Such a list would be passed from the ID Provider to the Relying Party in advance of providing the Verification service.

Auditing – ID Providers must submit to the entire Audit Process described herein. Separately, an ID Provider must also be able to provide an independent auditor with the TN and date-timestamp of queries requested by a Relying Party being audited. This information can be used by the auditor to verify that transactions submitted to the Relying Party or a Relying Party Reseller are submitted in turn to an ID Provider, the presumption being that a mismatch would be due to caching.

8.0 Relying Party Additional Responsibilities

Additional responsibilities of a Relying Party who is certified under this Trust Framework include the following.

Minimum Data Quality – A Relying Party must provide a minimum of telephone number, name and/or address in order for their service to be considered a certified Verification service. A Relying party must submit verification transactions via a standard interface and protocol such as XML or HTTP, HTTPS or SS7.

Auditing – A Relying Party must submit to the entire Audit Process described herein. Relying parties must be able to prove to an independent, third-party auditor the following:

- The Relying Party adheres to all requirements for certification under the Trust Framework
- The Relying Party follows industry best practices including, but not limited to
  - Following all legal, regulatory and contractual restrictions over the use of common telecom system data repositories including, but not limited to LIDB and CNAM.