i3Forum

Principles and best practice for mitigating fraudulent, illegal and unwanted communications

Know Your Customer / Know Your Traffic Code of Conduct

OCTOBER 2024

i3Forum

Table of Contents

Introduction

Know Your Customer (KYC) and Know Your Traffic (KYT) best practices and principles involve measures to authenticate and verify customer identities, conduct due diligence on their operations, compliance history, and other relevant factors crucial for assessing the risks of potential non-compliance with applicable laws and the associated liability for communications providers. The widespread and effective implementation of KYC is vital to reducing the criminal abuse of networks and enhancing the trust of customers.

The implementation of KYC procedures is not merely a voluntary option. It has become an explicit legal obligation mandated by laws and regulations around the world. Additionally, regulators around the world have emphasized KYC requirements in their enforcement proceedings. Failure to implement robust KYC procedures has resulted in significant fines, tarnished reputations, and the imposition of compliance plans with regular mandatory reporting.

Some regulators do not explicitly outline the steps a communications provider must take to learn about prospective customers and ensure services are not used to originate illegal traffic. However, adhering to industry standards in good faith is typically viewed favourably by regulators. The purpose of this document is to establish a general set of KYC best practices and principles for i3Forum members and the communications industry at large. The best practices speak largely to service relationships with legal entity customers (businesses and other organizations). KYC for individual consumer customers may involve similar principles but will require different practices.

We encourage all i3Forum members and other providers of communications services to pledge to follow this Code of Conduct to the fullest extent to which it can be applied to their business and its customers. This document will not capture every scenario or circumstance and does not constitute or convey legal advice. Businesses should consult their legal counsel for assistance and adopt KYC standards that reflect the services they provide, the jurisdictions in which they operate, and the customers they serve. Businesses should comply with any applicable legal or regulatory requirements in addition to the practices advocated by this Code of Conduct. These KYC best practices have been drafted with no specific legal jurisdiction in mind.

The remainder of this Code of Conduct describes KYC information that should be collected from prospective customers and methods of validating this information against authoritative sources for accuracy where available. Communications providers are encouraged to enhance the information below to better fit their circumstances or to improve their processes.

i3 Forum's draft Know Your Customer / Know Your Traffic Code of Conduct is based on Numeracle's Model Standards for Know Your Customer first published in 2023. i3 Forum has taken Numeracle's model standards and adapted them for international use and other forms of electronic communication. CCA has been an enthusiastic early proponent of rigorous KYC practices and has been a valuable contributor to promoting KYC adoption.

Policy Compliance

This Code of Conduct is not a policy to be copied unthinkingly but it provides a basis for communications providers to establish their own KYC and KYT policies whilst facilitating comparison with the practices adopted by others. The formal policy of each communications provider may deviate from this Code of Conduct where appropriate for the specific circumstances of the service being provided or the customer being served because not all current and future eventualities can be anticipated by a general purpose industry code like this one. However, there is a core of mandatory requirements. Where a communications provider has chosen not to follow one of the non-mandatory requirements of this code or has otherwise lowered the KYC and KYT standards that they apply in practice, then their corporate policy should document the justification for deviating from this code. The principle of 'comply or explain' allows flexibility in standards whilst placing the onus on businesses to transparently demonstrate their commitment to the goal of mitigating fraudulent, illegal and unwanted communications. For the avoidance of doubt, the 'comply or explain' principle does not apply to the core mandatory requirements.

All requirements in the Code of Conduct are equally important, but as some can be waived under the "comply or explain" principle, and given the nature of this industry where multiple suppliers service an initial customer along the call path, it is essential to identify a "core" set of KYC requirements that are non-negotiable (i.e. for which the "comply or explain" principle does not apply).

This is important for carriers further down the call path, who are not in contact with the initial customer (hence unable to perform their own KYC), but need to trust that the initial carrier's compliance with the KYC Code of Conduct for that customer guarantee that at least a minimum set of requirements have been met (and not waived).

Communications providers should educate their employees about the corporate KYC and KYT policy with the goal of ensuring the policy is followed consistently in real life. To further pursue this goal, each communications provider should identify at least one person who will have particular responsibility for upholding the policy. The duties of the KYC compliance leader and their team include:

- Performing pre-agreement reviews of all prospective customers to determine whether they meet the corporate KYC and KYT policy requirements, keeping documentation of all information considered, decisions reached, and all the individuals involved in the review.
- Performing escalated enhanced due diligence reviews and making KYC decisions for higher-risk clients identified through the standard review process.
- Ensuring corporate policy is sufficient to meet changes in legal and regulatory obligations and consulting with internal teams on legal questions that arise as part of KYC processes.
- Supporting the development or implementation of the tools, systems, or other resources needed to perform and document KYC and KYT in a timely manner.
- Working with line management and human resources management to ensure the adequacy of the KYC and KYT training that is given to staff.

KYC and KYT involve knowing about the customer, knowing about the use cases for their traffic, and knowing which jurisdictions apply to this traffic.

If information is collected using a form, and multiple use cases apply to one customer, then the customer should fill out a separate form for each use case. Voice and messaging are examples of separate use cases. No exhaustive list of use categories is given in this code as different categories may be suited to communications providers depending on which regions they mostly do business, and new use categories will be developed over time.

Customers should be asked to list each jurisdiction that will apply to the traffic described by each use case. It may be necessary to ask follow-up questions to ensure legal and regulatory compliance in some jurisdictions. To avoid complexity, this code does not contain examples of questions that are relevant to specific jurisdictions. However, a communications provider may choose to include such questions in the standard KYC/KYT forms they provide to customers prior to activation if they expect all or most of their customers and traffic will need to comply with the requirements of a specific country. For example, it is appropriate for a US carrier that mostly concentrates on terminating traffic in the USA to ask prospective customers about compliance with the specific wording of FCC regulations when it would be inappropriate for a carrier in another region to ask those same questions of a customer whose traffic does not terminate in the USA.

The core mandatory information for which the 'comply or explain' principle does not apply are marked with '*' in the lists below.

Information about the Customer

About the customer's lead contact

- Given name *
- Family name *
- Job title and department *
- Phone number *
- Email address (as consistent with company information requested below) *
- Address, including country *

About the customer's company

- Full legal name of company *
- A list of all business and trade names ('doing business as') used by the company during the last three years
- Country of incorporation and legal address *
- Physical address representing a real place of business associated with the entity that is not a virtual address, shared office location without a dedicated suite or floor, PO box, mail forwarding service, hosted server location, etc. (this will be checked using Google Street View or equivalent) *
- Billing address, if different to the above *

- Company registration number *
- Tax identification numbers as relevant (VAT, GST, EIN or similar) *
- URL of company website
- Company phone number *
- Company email address (the domain should match the website or be verified as belonging to the legal entity) *
- Type of business (select all that applies): wholesale / retail / cloud numbers / XaaS *
- Full legal name of parent company (companies) (if applicable)
- Country of incorporation and legal address of parent company (companies) (if applicable)
- Name(s), address(es), and email address(es) of all individuals with 10% or more direct or indirect ownership of the company
- Has the company, any parent companies, or any owners been subject to any criminal investigations or judgments for alleged illegal activity concerning services of the type listed in the use cases below?
- Has the company, any parent companies, or any owners been subject to regulatory sanctions or civil penalties concerning services of the type listed in the use cases below?
- Any KYC, KYT or similar policy that the customer's company applies to *their* customers

Information about Each Traffic Use Case

These questions should be separately answered for each distinct use case:

- The use case of the traffic: national or international; voice or messaging *
- A list of all jurisdictions that apply to international traffic *
- A description of legal and regulatory compliance practices applicable to the jurisdiction(s) and the services to be provided
- Evidence of a license or other legal authorizations required to convey traffic per the use case
- Type of customers served: (select all that applies): conference calling, call centre, enterprises, wholesale, mobile network operators, mobile virtual network operators, cable operators
- Whether the traffic is telemarketing; if yes, then a description of the traffic
- Trunk identification
- Expected traffic volume and origin
- A description of the procedure for obtaining the consent of recipients of calls, as applicable
- National CLI on international SIP trunks

The extent of checks to be performed to determine the accuracy of information provided by the prospective customers depends on the risks associated with the prospective customer's business model and traffic. The following KYC and KYT checks are appropriate for all kinds of customers and traffic for improved risk limitation.

Mandatory validations:

- Check if the use cases listed by the prospective customer are consistent with services described on their website.
- Verify that the physical address given for the prospective customer is a genuine place of business as opposed to a post office box, mail forwarding service, virtual address or an address is the same as that used by many other businesses. This can be done by online searches for businesses that use the address and by examining the building's location and appearance using Google Maps and Google Street View.

Recommended complimentary validations:

- Examine business registries to determine if the details associated with the prospective customer's corporation registration are consistent with the information they have provided about business activities, ownership, legal address etc.
- Make enquiries with credit agencies.
- Search for court cases, regulator reviews, and any other news indicative of the prospective customer having a bad reputation.
- Review the adequacy of the KYC and KYT policies of prospective customers who are also communications providers that need to check the authenticity of their customers and traffic.
- Identify any gaps in the prospective customer's answers about compliance practices for traffic where there are known to be particular requirements imposed by the jurisdictions listed for that traffic.

The review may indicate that the risk of onboarding a new customer only becomes acceptable if specific additional risk mitigations are undertaken. These should be fully documented, and internal audits should periodically confirm the documented risk mitigations are executed in practice. Examples of additional risk mitigation include the following.

- The imposition of limits on the new customer's traffic volumes/capacity or expenditure.
- Only permitting the customer to obtain lower-risk services.
- Enhanced monitoring of the new customer's activity.
- Explicit penalty fees in the customer's contract.
- The customer may not make changes to their service without heightened levels of approval from the management team of the communications provider.

The following are some of the potential indicators that a prospective customer represents a heightened risk.

- Telemarketing.
- The customer operates in a specific jurisdiction, wishes to use numbers associated with a different jurisdiction, but there is a lack of evidence that the customer is authorized to use those numbers.
- IT support call centres not owned/operated/staffed by the business which manufactured or provides the IT product or service.

- The location of the prospective customer's head office, management team or staff is in a different jurisdiction to the people and organizations they want to communicate with.
- The ownership of the prospective customer is obscure or part of a complicated web of legal entities.
- There is no evidence that the business is a registered legal entity.
- The prospective customer is unwilling to provide information.
- When questioned, the prospective customer provides answers that are vague or incomplete.
- Staff working for the prospective customer are hostile when questioned.
- There is pressure to urgently complete the pre-activation review.
- Email addresses used by the prospective customer reflect a variety of different business entities or use generic domains like Gmail.
- Emails sent to the prospective customer bounce.
- Calls made to the prospective customer's phone number are rarely or never answered.
- The prospective customer's staff are unwilling to speak over the phone.
- The prospective customer's staff keep avoiding, postponing and cancelling meetings.
- The prospective customer's website is incomplete or new.
- Information and documentation supplied by the prospective customer is unprofessional, incomplete or new.
- Searches show the prospective customer has been the subject of adverse court judgments, complaints, or other indicators of a bad reputation.
- The prospective customer is unaware of compliance obligations in the relevant jurisdictions or cannot explain how they comply with them.
- Where it is necessary to show that recipients have consented to the traffic they receive, the prospective customer is unable to show how consent was obtained.
- Where the prospective customer is a communications provider, they cannot explain how their KYC and KYT policies were applied to the relevant traffic.
- The amount of the proposed traffic is unusually large relative to the time the prospective customer has been in business, the number of staff they employ, or the quality of their web presence.
- The prospective customer seeks a detailed breakdown of how the communications provider makes KYC and KYT decisions.

None of the lists above should be considered exhaustive. The KYC compliance lead and their team should have discretion to extend and adapt their work to reflect the risks posed by different prospective customers and different kinds of traffic.

Post-Activation Monitoring and Reviews

All customers should be monitored for suspicious traffic. The following data should be regularly captured and assessed.

- Reports of alleged improper communications sent from downstream communications providers, the general public, or others.
- Data on consumer complaints filed with government agencies or other relevant organizations.
- Requests for high capacity (calls per second or concurrent calls), particularly if disproportionate to the size of the account.
- Traffic statistics, including:
    - short call duration percentage;
    - average call duration;
    - answer seizure ratio (ASR);
    - the percentage of call attempts blocked due to an improper CLI (invalid, unallocated, on a DNO list etc);
    - delivery receipt ratio (DLR);
    - ratio of long code Sender IDs relative to short code Sender IDs; and
    - ratio of long code Sender IDs relative to alphanumeric Sender IDs.

Customer accounts should regularly be reviewed for compliance with the KYC and KYT policies and with the compliance obligations of each pertinent jurisdiction. Scheduled reviews that confirm all information is up to date and the extent to which risk profiles may have altered can occur on a quarterly or annual basis, or according to the contract renewal cycle. Reviews may also be triggered by the following circumstances.

- The customer advises a change to the KYC information provided previously.
- The customer seeks approval for higher-risk products, higher capacity, a nonstandard use case etc.
- The traffic exceeds or nears a threshold or limit for the service being provided.
- There have been complaints about a customer or their traffic.