2024

Cloud Communications Alliance

Numeracle

Cloud Communications Alliance & Numeracle

KNOW YOUR CUSTOMER "KYC"

Principles & Best Practices

www.numeracle.com
www.cloudcommunications.com

PREPARED BY

Numeracle

Table of Contents

Introduction

As the leading peer association committed to advancing the Cloud Communications industry, the Cloud Communications Alliance (CCA) is dedicated to educating our members on regulatory compliance requirements and shaping top-tier industry standards. Our mission at the CCA is to nurture the integrity, security, and outstanding performance of Cloud Communications systems, fostering confidence and trust between callers and receivers ("Trust in Networks").

Know Your Customer ("KYC") 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 service providers ("CSPs"). The widespread and effective implementation of KYC by CSPs is pivotal in enhancing overall Trust in Networks.

It is crucial to highlight that the implementation of KYC procedures is now not merely a voluntary option but rather an explicit legal obligation mandated by applicable laws and regulations around the world. Additionally, regulators around the world have emphasized this requirement in their enforcement proceedings. Failure to implement robust KYC procedures has resulted in significant fines, tarnished CSP reputations, and the imposition of compliance plans with regular mandatory reporting.

While some regulators do not explicitly outline the steps a CSP must take to meet the requirement the US Federal Communications Commission ("FCC") describes as "knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic,"[1] adhering to industry standards in good faith is typically viewed favorably by regulators. The purpose of this document is to establish a general set of KYC best practices and principles for CCA members and the communications industry at large, to follow when commencing service for customers and throughout the customer relationship. The best practices speak largely to service relationships with legal entity customers (businesses and organizations). KYC for individual consumer customers may involve similar principles but will require different practices.

1 *Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, Fourth Report and Order, https://docs.fcc.gov/public/attachments/FCC-20-187A1.pdf*

We encourage all CCA members and members of the communications industry at large to pledge to implement these KYC best practices and principles and to encourage their partners and service provider customers to implement them as well. Adoption and use of these best practices and principles reflects a company's commitment to preclude the use of its network(s) to transmit illegal or unwanted calls or traffic while providing the highest quality communications service to its customers. CCA members who pledge to comply with these KYC best practices and principles will receive a special designation as a "CCA KYC member."

These KYC Best Practices and Principles apply when providing service to both:

Communicating End Entities ("CEEs")

A legal entity whose employees directly initiate or receive communications. CEEs include both entities initiating communications on their own behalf and companies that provide outsourced call center services where employees initiate, or answer calls on behalf of another company.

Communications Service Providers ("CSPs")

A legal entity whose products or services enable other businesses to initiate or receive communications.

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 fit their organization. Use of these best practices and principles does not create an attorney-client relationship with CCA. To the extent any governing regulatory authority mandates KYC policies or practices different from or exceeding these best practices and policies, CCA member companies will comply with any such regulatory requirements.

These KYC best practices have been drafted with no specific legal jurisdiction in mind. Companies that adopt KYC polices should be aware that some jurisdictions may have mandated KYC requirements that are stricter or more granular than those outlined herein. Nonetheless, the KYC procedures outlined in this document largely reflect KYC principles and serve as a satisfactory initial reference point.

CCA wishes to express its gratitude to Numeracle which designed the framework underpinning these principles and best practices and CCA members, Marashlian & Donahue, PLLC ("The CommLaw Group") and Brownstein Hyatt Farber Schreck, LLP, for supplementing them with precedential insights and other applicable legal considerations. [2]

We recommend that companies adopting KYC policies and best practices contact experienced and specialized legal counsel for assistance in reviewing and implementing their KYC program.

[2] *Disclaimer: The content provided herein may be considered attorney advertising in certain jurisdictions. Such advertising is subject to rules and regulations that vary by location. The information presented is for informational purposes only and should not be construed as legal advice or the establishment of an attorney-client relationship. Prior to making any legal decisions, it is advisable to consult with an attorney in your jurisdiction to discuss your specific legal needs and circumstances. Viewing this content does not create an attorney-client relationship, and any communication through this platform should not be considered confidential or privileged. The choice of a lawyer is an important decision and should not be based solely on advertisements.*

Know Your Customer Policy Compliance Designation & Duties

Companies that adopt KYC policies should educate their employees about these policies, identify individuals that will have particular responsibility for upholding those policies and designate a KYC Compliance Lead who will be fully responsible for the company's KYC Policy and programs. The duties of the KYC Compliance Lead include overseeing policy implementation and updates, monitoring policy compliance, and employee training.

Companies may identify additional individuals or teams (collectively, the KYC Compliance Team) to assist the KYC Compliance Lead in managing, coordinating, and adhering to KYC Policy. The organization, titles, and management of such team(s) may vary depending on the structure of the company.

The responsibilities of the Compliance Lead and the KYC Compliance Team should include:

- Performing pre-agreement reviews of all prospective customers to determine whether they meet company KYC Policy requirements, keeping detailed documentation of all information considered, decisions reached, and the individuals involved in the review.
- Performing escalated enhanced due diligence reviews and making KYC decisions for higher-risk clients identified in the standard review process.
- Ensuring that company KYC Policy sufficiently meets any applicable legal obligations and adequately addresses legal risks, including consulting with internal teams on legal questions that arise as part of KYC processes.
- Supporting the development or implementation of the tools, systems, or vendor resources needed to perform and document KYC processes in a timely and scalable manner.

Pre-Activation Review

3.1 Verified Identity Program

The following information should be collected from customers and validated against authoritative sources for accuracy where available. CSPs are encouraged to enhance the below to better fit their circumstances or to improve their processes.

a. Full legal name
b. State/Province/Country of Incorporation
c. Entity tax identification number (EIN, VAT, or similar)[2]
d. Entity registration number
e. 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. An employee will view the address in Google street view or equivalent to verify.
f. Billing address, if different
g. Entity's parent company(ies) legal name(s) (if applicable)
h. Entity's parent company(ies) state/province/country of business incorporation (if applicable)
i. Entity's website(s)
j. Name(s), address(es), and email address(es) of all individuals with 10% or more direct or indirect ownership of the entity
k. A list of all business and trade names, DBAs and related websites under which the customer has transacted business for the previous three (3) years.
l. Collection and validation of a contact email address with a domain name that exactly matches the entity website provided or a domain verified as controlled by the entity. Care should be taken to detect impersonation attempts using similar domain names or email account takeover.

Additional details for Communication Service Provider ("CSP") customers:

a. Identifier(s) sufficient to verify any required registration(s) (or as desired, optional registration(s)) with governmental authorities overseeing telecom services in the country(ies) in which services will be provided.
    a. For example, in the United States this may include:
        i. Active Robocall Mitigation Database information including entity's FCC Registration Number (FRN) and Robocall Mitigation Database (RMD) ID (if applicable)
        ii. FCC Form 499 Filer ID Number (if available)

2 *Legal entities such as sole proprietorships in the US may not have a separate business tax identifier. CSPs may consider performing additional risk-based analysis of such entities to enable services where appropriate without allowing customers to improperly undergo a lower level of KYC review.*

Pre-Activation Review

3.2 Understanding Intended Use & History

Performing customer KYC requires an understanding of customers' intended use of services. The following materials should be collected and reviewed prior to service activation.

All customers:

a. A description of the intended use of services
b. Entity's website and public-facing materials
    i. Legal entity customers should have an active, dedicated web domain that meaningfully describes the nature of the entity's business and services. The entity's webpage and social media should also be used to assess reasonable business establishment (are there significant broken links, placeholder text, etc.), company leadership details, stated office locations, any published policies or processes, etc.
c. The full set of products and services that will be enabled upon activation.
d. A certification of whether the entity or its owners have been subject to any prior enforcements or judgments for alleged illegal activity related to itself or related entities and, if so, provide details
e. An active review of potentially negative reputational material including law enforcement actions, regulatory sanctions, or civil judgements.

Additional details for Communicating End Entity ("CEE") customers:

f. A description of the calls to be made
g. A description of consent collection practices
h. A description of legal compliance practices applicable to the jurisdiction(s) in which services are being provided. For example, In the United States, the Telephone Consumer Protection Act (TCPA), Truth in Caller ID Act, and Fair Debt Collection Practices Act (if applicable)

Additional details for Communication Service Provider ("CSP") customers:

i. Confirmation of whether the CSP supports CEE customers (legal entity or consumer), CSP customers, or both, and how the CSP proactively verifies or controls for CEE vs. CSP customer categorization
j. The CSP's signup and KYC processes
k. Products and services marketed/offered

All data or communication collected and reviewed as part of verifying the identity or understanding the intended use and history should be documented and preserved in internal records such that future reviewers can determine what was reviewed or verified, any conclusions drawn, and the individual(s) that conducted the review.

Pre-Activation Review

3.3 Proactive Establishment of CEE vs. CSP Categorization

CEE and CSP customers represent different potential risks and regulatory considerations, and it is critically important to understand the nature of the customer's business(es). Many businesses may have incorporated communications services into their own offerings despite not self-identifying as a CSP.

As part of its KYC review process, a CSP should proactively evaluate whether a customer appears to be operating as a CSP or a CEE. While customer-provided information may be taken into account, KYC teams should not rely on a customer's own designation of whether it is a CSP or CEE.

Team members should review the information provided by the prospective customer as well as its website and public materials to confirm if it appears to be a CSP.

3.4 Enhanced Due Diligence

For any entities that may represent a higher level of risk (as described in Section 6. Criteria Prompting Enhanced Due Diligence of this document), additional steps should be taken to review, monitor, and restrict accounts. Accounts in this category should require approval by responsible individual(s) ("KYC Leader(s)"). The KYC Leader(s) should confirm whether a customer can be approved.

If not denied outright, the KYC Leader(s) should determine and apply additional appropriate risk mitigation measures. Potential risk mitigation measures may include but are not limited to actions such as additional customer activity monitoring, volume/capacity/spend limitations, restricting access to higher-risk products or services, penalty fees or agreement terms, or requiring KYC Leader approval for account changes.

The results of Enhanced Due Diligence should be fully documented and preserved to ensure the results are captured and any risk mitigation measures are appropriately applied to the customer account.

Post-Activation

4.1 Activity Monitoring

All customer accounts should be monitored for potentially unusual or suspicious usage. The following metrics should be monitored:

- Reports of alleged improper communications sent to the CSP from downstream CSPs, the general public, or others.
- Data related to consumer complaints filed with governmental agencies or other relevant organizations
  - In the United States, this would include sources such as Traceback requests, complaints filed by consumers with the FCC or FTC, etc
- Call traffic statistics
  - Short call duration percentage
  - Average call duration
  - Answer Seizure Ratio (ASR)
  - Percentage of call attempts blocked due to improper caller ID (invalid, unallocated, on a DNO list) if applicable
- Requests for high capacity (calls per second or concurrent calls), particularly if disproportionate to the size of the account

4.2 Further KYC Reviews

Customer accounts should be reviewed under the KYC Policy on an ongoing basis. Reviews can be inserted throughout the customer lifecycle using methods such as:

- Approval gates - Required approval for changes to business information or access to specific higher-risk products, high capacity, nonstandard use, etc.
- Triggered reviews - Thresholds and/or alerts for use, changes in use, disproportionate complaints, account changes, etc.
- Reporting - Global monitoring of customer activity; and
- Scheduled Reviews - Reconfirming account information and reviewing activity on a regular, scheduled basis. This could be performed based on the calendar year (quarterly, annually, etc.) or during a contract renewal cycle.

10

Trial Accounts

CSPs should strongly consider not providing customers with access to communications to/from the larger phone network without first undergoing a full KYC review and approval. All trial accounts should be time-restricted, with any extension requiring approval by KYC Leader(s).

To gain access to a trial account, customers should undergo either a full KYC review or, at a minimum, the collection, review, and approval of the following (subject to full KYC review prior to conversion to a regular account):

- Full legal name
- State/Province/Country of Business Incorporation
- Physical address representing a real place of business associated with the entity.
- Entity's website(s)
- Entity contact name for the trial account.
- Collection and validation of a contact email address with a domain name that exactly matches the entity website provided or a domain verified as controlled by the entity.

CSPs should limit the usage of trial accounts to ensure customers are not given access to/from the larger phone network without a full KYC review.

Trial account usage should be closely monitored to ensure that 1) accounts are properly reviewed prior to activation and promptly deactivated upon expiration of the trial period, and 2) that trial account usage is not unreasonable, unexpected, abusive, or fraudulent. Should inappropriate use be found, the offending trial accounts should be terminated immediately.

Criteria Prompting Enhanced Due Diligence or Rejection

6.1 High-Risk Categories

Accounts associated with the following industries or business models have a higher risk of carrying highly regulated, unsolicited, or potentially illegal communications. While many legitimate operators may be in these categories, many have been subject to enforcement actions.

Customers in these categories or who serve businesses in these categories require a higher standard of KYC review.

- Affiliate marketing/lead generation
- High-risk financial services (payday loans, debt relief, credit repair, auto/home warranties, loan offers by non-direct lenders, etc.)
- Third-party debt collections
- Political communications, fundraising (political or nonprofit), surveys
- IT support call centers not directly staffed and operated by the device or software manufacturer.
- Highly marketed services (solar power, for-profit colleges, etc.)
- Businesses seeking US-based communications services that have a physical location in the United States but whose headquarters, staff, or leadership are located primarily outside of the United States.

Criteria Prompting Enhanced Due Diligence or Rejection

6.2 Red Flag Behaviors

The following behaviors should be considered indications of potential high risk if observed before, during, or after customer activation and should prompt enhanced due diligence or, potentially, rejection or termination of the account.

- Unwillingness or expressions of hardship to provide requested information (or an unexpected eagerness to provide information)
- Aggressive, hostile behavior or over-escalation
- Claiming very large amounts of traffic with no clear basis (very few employees, brand new business entity, no web presence outside of a company website, etc.)
- Vague or incomplete answers to questions
- Unsolicited, notable interest in specific KYC processes and criteria
- Creating pressure to complete an agreement as soon as possible
- Customer's business entity is associated with a large number of related businesses or a complex structure of ownership without a clear reason
- Communication using email domains associated with multiple businesses or using public email domains (gmail, hotmail, etc.)
- Customer is unwilling to speak over the phone or repeatedly avoids, cancels, or postpones meetings
- Customer presents as operating in one location but all customer contacts and operations seem to be located elsewhere or contacts claim to be traveling elsewhere

6.3 High-Risk Findings

CSPs should consider it to be an indication of high risk prompting enhanced due diligence or, potentially, rejection or termination of the account, especially if combined with other red flags behaviors or high risk categories if before, during, or after a KYC review of a customer:

1. Has refused to provide or is otherwise unable to provide applicable information or documentation listed in 3.1 and 3.2 above or as otherwise required under the CSP's KYC policy, including, but not limited to:
    (1) Does not have an active website that describes its products or services, or has a website or public social media page that presents obvious indicia of fraud;
    (2) Does not have a verifiable email address with the same domain as its website; or
    (3) Does not have a verifiable physical address as described in 3.1(e).

2. Has reported and, if requested to correct, has not corrected incomplete, false, inaccurate, or misleading material information, including, but not limited to:
    (1) Providing mismatching information across sources, including the customer's website, business registration/licensing records, and regulatory filings, as applicable; or
    (2) Providing inactive or false means of contact, including email addresses, phone numbers, and mailing addresses.

3. Is not able to be found as an actively registered business or other legal entity in good standing with the state, province, country, or other jurisdiction of its principal place of business.

4. Provided information, website, or documentation is unclear, incomplete, unprofessional, or appears to have been created very recently.

5. Is found to have been the subject of relevant, material, and adverse legal or reputational findings such as civil or criminal judgments, other regulatory enforcement actions, or a significant and disproportionate number of informal consumer or CSP complaints related to communications it has initiated or enabled.

6. Customer or customer's customers do not appear to obtain sufficient consent for communications as required by applicable law or the reviewing CSP's usage policy(ies).

7. Customer's account activity or call traffic statistics are inconsistent with previous statements or with typical customer use, and:

   (1) Some or all customer activity appears to be illegitimate, unlawful, or harmful,

   (2) The customer's previous representations appear to have been knowingly or negligently false or misleading; or

   (3) Customer activity has resulted in or is likely to result in complaints from communication recipients.

8. If a CSP, the customer does not appear to have sufficient processes, policies, and/or resources to conduct its own customer KYC.

The above should not be considered an exhaustive list and CSPs should provide their KYC Compliance Teams with sufficient authority and independence to assess risk and determine appropriate treatment under the guidance of the KYC Leader(s) and the CSP's KYC Policy.

KNOW YOUR CUSTOMER

Principles & Best Practices

About Numeracle

Numeracle's Entity Identity Management Platform and Verified Identity platform enable legal entities to prepare for STIR/SHAKEN, prevent improper call blocking and 'Fraud' labeling, and employ best practices to prevent 'Spam' labeling by working with tech providers, carriers, device manufacturers, & analytics companies, providing visibility and brand management across the telecom ecosystem.

Direct Inquiries
Numeracle Sales
sales@numeracle.com

Contact the Author
Sarah Delphey
VP of Trust Solutions
sarah.delphey@numeracle.com

Numeracle

About The Cloud Communications Alliance (CCA)

The Cloud Communications Alliance is the world's premier peer association dedicated to the growth of the Cloud Communications industry. The CCA is comprised of executives from cloud communication companies. The alliance provides executive leaders from all over the wold with a forum to come together and discuss key topics and trends.

Cloud Communications Alliance