

Know Your Customer Policy, Procedures and Robocall Mitigation Plan

Dominion Cup Telecom Canada Inc (“Dominion”) is committed to maintaining robust policy around the Know Your Customer (“KYC”) process. This policy and process strives to identify customer entities effectively in an effort to prevent and mitigate noncompliant and illegal activity on Dominion’s network and serves as Dominion’s robocall mitigation plan. The following policies and procedures (“KYC Policy”) relates to customers placing a significant number of outbound calls with destinations in the United States.¹

1. Know Your Customer Policy Compliance Designation and Duties

All employees are responsible for acting in accordance with KYC Policy. The following individual(s) and team(s) have specific responsibilities for upholding KYC Policy:

The Compliance Lead is responsible for the company’s KYC Policy and programs. The duties of the Compliance Lead include overseeing policy implementation and updates, monitoring policy compliance, and employee training.

The KYC Compliance Lead will manage KYC Policy adherence in coordination with the following teams and individuals:

Compliance Lead:

- Leader: Gabrielle Rife
- Responsibilities:
 - Will perform reviews of prospective customers to determine whether they meet company KYC Policy requirements, keeping documentation of information considered and decisions reached.
 - Will perform enhanced due diligence reviews and make KYC decisions for any customers identified in the standard review process that may require heightened scrutiny.
 - Responsible for ensuring that company KYC Policy sufficiently meets any applicable legal obligations. Will consult with internal teams and, when necessary, external legal counsel on questions that arise as part of KYC processes.
 - Responsible for supporting the development or implementation of the resources needed to perform and document KYC processes in a timely and scalable manner.

2. Pre-Activation Requirements

¹ The Compliance Lead at times innovates and explores alternative KYC processes and/or documents as appropriate to the circumstances of specific customers.

Verified Identity Program

The following data should be validated against authoritative sources for accuracy where available.

- Full legal name
- State/Province/Country of Business Incorporation
- Secretary of State registration or Employer Identification Number (EIN) or equivalent international information
- Physical address representing a real place of business associated with the entity
- Entity's parent company(ies) legal name(s) (if applicable)
- Entity's parent company(ies) state/province/country of business incorporation (if applicable)
- Entity's website(s)
- Contact email address²

Understanding Intended Use & History

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

Customers other than Communication Service Provider ("CSP")³ customers:

- Know Your Customer Questionnaire (Standard)
- Acceptable Use Policy

CSP customers:

- Know Your Customer Questionnaire (Provider)
- Acceptable Use Policy
- The CSP's KYC policy and/or procedure and/or terms and conditions for their customers or the applicable Know Your Customer Questionnaire for each entity sending traffic to the Dominion network.

Data or communication collected and relied upon 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.

Proactive Establishment of CSP Categorization

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

² Typically, the domain name should match the entity website provided or a domain verified as controlled by the entity, parent company, or associated company.

³ Communications service providers ("CSPs") - A legal entity whose products or services enable other businesses to initiate or receive communications.

CSP. Therefore, Dominion will use information gathered during the KYC process to help evaluate whether a customer appears to be operating as a CSP.

Enhanced Due Diligence

For any entities that the Compliance Lead deems eligible for enhanced due diligence after completing the standard review process, additional steps may be taken to review, monitor, and restrict accounts. Accounts in this category will require approval by the Compliance Lead. If approved, the Compliance Lead will determine if additional risk mitigation measures are necessary to service the account.

3. Post Activation

Activity Monitoring

Customer accounts will be monitored for potentially unusual or suspicious usage.⁴ The following metrics will be monitored:

- Traceback requests
- Reports of alleged improper communications sent to Dominion from downstream providers, the general public, or others
- Subpoena or other regulatory body requests sent to Dominion
- Calls with an improper caller ID (such as on a Do Not Originate list)

Further KYC Reviews

At the discretion of the Compliance Lead, Customer accounts may be reviewed under the KYC Policy based on events logged from the above Activity Monitoring or other events.

4. Related Policies and Procedures

Response to Traceback Requests

Dominion takes seriously any request from the FCC, law enforcement, the industry traceback consortium, and other regulatory entities and will fully cooperate with such entities in investigating and stopping illegal robocallers that use its service within 24 hours of receipt of such request.

⁴ Dominion does not use data analytics as a part its Robocall Mitigation Plan.