Know Your Customer Policy, Procedures and Robocall Mitigation Plan

Broadband Dynamics Canada Telecom and Software, ULC ("BBD Canada") 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 BBD Canada's network and serves as BBD Canada'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:

Robert Rife is the company's KYC Compliance Lead and 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 Committee

- Leader: Robert 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 supporting the development or implementation of the resources needed to perform and document KYC processes in a timely and scalable manner.

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

- 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.

2. Pre-Activation Requirements

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 website(s)
- Contact email address[2]
- Entity's parent company(ies) legal name(s) (if applicable)
- Entity's parent company(ies) state/province/country of business incorporation (if applicable)

Understanding Intended Use & History

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

Upstream Provider/Communication Service Provider ("UPCSP")[3] customers:

- Know Your Customer Questionnaire (Provider)
- Acceptable Use Policy
- The UPCSP'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 BBD Canada network.

[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] Upstream Provider/Communications service providers ("UPCSPs") - A legal entity whose products or services enable other businesses to initiate or receive communications.

Customers other than UPCSP customers:

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

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.

The Service Agreement and its associated Terms and Conditions customers sign states the customer will comply with all applicable laws and the Acceptable Use Policy.

Proactive Establishment of UPCSP Categorization

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

Enhanced Due Diligence

For any entities that the Compliance Committee 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 Committee. If approved, the Compliance Committee 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. The following metrics will be monitored:

- Traceback requests

- Reports of alleged improper communications sent to BBD Canada from downstream providers[4], the general public, or others
- Subpoena or other regulatory body requests sent to BBD Canada
- Calls with an improper caller ID (such as on a Do Not Originate list)

Further KYC Reviews

At the discretion of the Compliance Committee, 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

BBD Canada 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] BBD Canada does not directly use data analytics as a part its Robocall Mitigation Plan. Instead, BBD Canada relies upon our wholesale voice carriers data analytics for this aspect of monitoring.



Broadband Dynamics Canada Telecom and Software, ULC Acceptable Use Policy

This Acceptable Use Policy ("AUP") describes actions that Broadband Dynamics Canada Telecom and Software, ULC ("BBD Canada") prohibits when any party uses its Services. By ordering or using BBD Canada's Services, you, the Customer or service recipient, agree to the terms of this AUP. Each Customer must review and comply with this AUP and all applicable laws, but this AUP is not intended to be interpreted as, relied upon, or used as a substitute for legal advice. You agree not to use, and not to encourage or allow any end user or other party to use, BBD Canada's Services in unlawful or prohibited manners, including, but not limited to, the following:

- Using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading, or any activity that exploits, harms, or threatens to harm children.
- Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services, including without limitation, any activities that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, all federal and state Do Not Call, calling-time, and call-quantity restriction laws and regulations.
- Using BBD Canada's Services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices and Short Code Monitoring Handbook.
- Attempting to bypass or disable any security mechanism on any of the Services or using the Services in any other manner that poses a security or service risk.
- Reverse-engineering the Services for any improper purpose.
- Using the Services in any manner that may subject BBD Canada or any third party to liability, damages, or danger.
- Launching or facilitating a denial-of-service attack on any of the Services or any other conduct that adversely impacts the availability, reliability, or stability of the Services.
- Transmitting any material that contains viruses, trojan horses, worms or any other malicious or harmful programs.
- Using the Services to receive, send or otherwise process Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996, as amended, unless you have signed a Business Associate Agreement with BBD Canada or your use of the Services fits within an exception for requiring a Business Associate Agreement.
- Using the Services to store or save credit card information, financial account information, social security numbers, or other information that could be used for fraud or identity theft.
- Using the Services to transmit any material that infringes the intellectual property rights or other rights of third parties.
- Using the Services to transmit any material that is libelous, defamatory, discriminatory, or otherwise malicious or harmful to any person or entity.
- Creating a false identity or forged email address or header, or phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act, 47 U.S.C. § 227, and implementing regulations, 47 C.F.R. § 64.1600 et seq., or using the Services to facilitate a one-ring scam, as the FCC has defined that term (*see* Report and Order, GC Docket No. 20-93; rel. Nov. 30, 2020).

- Transmitting any data to or through BBD Canada unless Customer represents and warrants that it has obtained and will maintain all necessary licenses, authorizations, approvals and consents to use, transmit, and process any data to or through BBD Canada during and/or in the use of the Services.

This list of prohibited uses is meant to be illustrative and should not be considered exhaustive. All determinations related to violations of this Acceptable Use Policy will be made by BBD Canada in its sole, reasonable discretion. BBD Canada reserves the right to change or modify the terms of the AUP at any time, effective immediately when posted to the BBD Canada website or when BBD Canada notifies you via an invoice insert. Customer's use of the BBD Canada Services after changes to the AUP are posted to the BBD Canada website or sent via an invoice insert shall constitute acceptance of any changes or additional terms. If you have a complaint about abuse or a breach of this AUP, please contact a BBD Canada representative.

If you violate these Terms, we may stop providing Services to you or we may close your account. We may also block delivery of a communication (such as a telephone call or SMS) to or from the Services in an effort to enforce these Terms. You also understand and agree that we are authorized and required to cooperate with and respond to all lawful civil, criminal, and regulatory inquiries relating to your use of the Services, including, without limitation, Traceback and other legal requests or demands from the FCC, FTC, civil and criminal law enforcement, and the FCC-designated USTelecom Industry Traceback Group consortium or any such successor entity. You also understand and agree that, pursuant to your contract with BBD Canada, you agree to defend, indemnify and hold BBD Canada harmless for any claims, demands, suits or proceedings alleging that you have violated the terms of this AUP or your agreement with BBD Canada. When investigating alleged violations of these Terms, BBD Canada reserves the right to review the content of your communications in order to resolve the issue. But we cannot monitor the entire Services, and make no attempt to do so.

_____
Company name

_____
Authorized company representative name

_____
Title

_____
Signature

_____
Date