

Group Shared Services

Robocall Mitigation Plan



Document #	USF-0000005
Document Custodian	David Miller - Head of Security
Reviewed by	Reviewed & Approved by
Date of last version issue (if applicable)	
Date of new issue	December 2024
Next review date	December 2025
Version #	1.0
Hierarchy Ref	Business

Foundation

- Global policies, procedures, and documents at the core of the Company's strategic directive
- Reviewed by key stakeholders and Approved by the CEO and/or senior leadership team

Management

- Global policies, procedures, and documents that govern the management of internal processes
- Reviewed by key stakeholders and Approved by senior management of the function area

Business

- Region specific policies, procedures, and documents that govern local work practices
- Reviewed by key stakeholders and Approved by senior management of the function area

1. Summary

Our Robocall Mitigation Plan (RMP) covers the controls that Vix implements to mitigate Robocalls and Spam calls as part of the voice services that we provide our US customers. The RMP also helps to show how we support actions taken by the Federal Communications Commission (FCC) to reduce Robocalls as well as our commitment to protecting our customers.

The Federal Communications Commission (FCC) requires all voice service providers to file certifications in the Robocall Mitigation Database regarding their efforts to fight illegal robocalls on their networks. Unwanted calls—including illegal and spoofed robocalls—are the FCC's top consumer complaint and a top consumer protection priority.

In addition voice service providers must describe their affirmative, effective measures to prevent customers from originating illegal robocalls.

Non-gateway intermediate providers and voice service providers must describe their know-their-upstream-provider program.

All providers must describe any call analytics systems they use to identify and block illegal robocalls, including whether they use a third-party vendor and the name of the vendor(s).

All mitigation plans must be provided in PDF.

2. Policy Purpose

This policy details our robocall mitigation plan as well as detailing the specific reasonable steps that we as the voice service provider have taken to avoid originating, carrying or processing illegal robocall traffic.

3. Scope

This policy applies to our Trachmar and IVR systems covering our US customers for external phone calls.

4. Definitions

- RMP - Robocall Mitigation Plan
- RMD - Robocall Mitigation Database - link to Vix registration - https://fccprod.servicenow.services.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robotcall_mitigation_database&sys_id=1de634f81b2e9150e4ccdb1de54bcbcd&view=sp
- FCC - Federal Communications Commission
- Trachmar - third party call centre that is used to support our customers
- IVR - voice call system used to support our customers
- 3CX - VOIP call software
- TRACED Act - Telephone Robocall Abuse Criminal Enforcement and Deterrence Act

5. Robocall Mitigation Database (RMD)

Through the Robocall Mitigation Database, voice service providers must certify whether and to what extent they have implemented the STIR/SHAKEN caller ID authentication framework.

Many voice service providers implement caller ID authentication throughout their networks. Those that do not must certify that they are implementing robocall mitigation practices and detail in the database the specific reasonable steps they are taking to avoid originating illegal robocall traffic.

Vix Technology (USA) Inc is registered as a Voice Service Provider within the RMD, however, Vix does not currently act in this capacity for the call centers it currently manages. We are not a voice service provider but we are still responsible for the call center's operations, ensuring compliance with applicable guidelines and regulations.

The online RMD certification form requires additional information. (This is why existing filers are required to update their certification.) The additional information to be collected includes:

- Detailed information about any claimed STIR/SHAKEN implementation extension or exemption - *Can be found in **Section 6 STIR/SHAKEN Framework***
- The role(s) the provider plays in the call chain - *Can be found in **Section 9 Systems in Scope - Role(s) Provider Plays In The Call Chain***

- Information about principals, affiliates, subsidiaries, and parent companies - *Can be found in the below table for reference.*
- A statement about whether the filer is subject to official action or investigation due to suspected unlawful robocalling or spoofing
 - At the time of writing (18/12/2024) Vix has not been subject to official action or investigations due to suspected unlawful robocalling or spoofing.
- The filer's Operating Company Number (OCN) - *Currently this is not something Vix has.*

The following are the details that Vix has registered with as part of our filing:

Last updated: December 2024

Robocall Mitigation Database Number	FCC Registration Number (FRN)	Business Name	Business Address
RMD0012409	0032976250	Vix Technology (USA) Inc	200 E. 5th Street, Suite 301, Tempe AZ 85281
Foreign Voice Service Provider	Other FRNs (enter 'None' if you have none)	Principals, Affiliates, Subsidiaries, and Parent Companies	Other DBA Name(s) (enter 'None' if you have none)
No	None	Vix Holdings Pty Ltd.	None
Previous Business Names (enter 'None' if you have none)	Robocall Mitigation Contact Name	Contact Title	Contact Department
None	David Miller	Head of Security	Compliance
Contact Business Address	Contact Telephone Number	Contact Phone Extension	Contact Email
200 E. 5th Street, Suite 301, Tempe AZ 85281	206-749-5500 206-577-3438	N/A	compliance@vixtechnology.com
Operating Company Number (OCN)			

6. STIR/SHAKEN Framework

STIR/SHAKEN is a framework of interconnected standards. STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards.

This means that calls traveling through interconnected phone networks can have their caller ID "signed" as legitimate by originating carriers and validated by other carriers before reaching consumers. STIR/SHAKEN digitally validates the handoff of phone calls passing through the complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is in fact from the number displayed on Caller ID.

STIR/SHAKEN framework does not apply to Vix Technology as an end user consumer however this is something that applies to our Voice Service Providers and is managed by them. Vix Technology works closely with our Voice Service Providers to ensure all applicable laws and regulations are met.

7. Systems in Scope - Overview

3CX

We use the 3CX phone system exclusively for **manual**, one-to-one calls. It is **not** employed for robocalling, autodialing, or any form of telemarketing. Additionally, because all inbound and outbound calls flow through our **third-party voice service provider**, we do not manage or control the underlying SIP trunks or PSTN connections. Below is an overview of our 3CX security and mitigation measures:

1. Global IP Blacklist

- We enable 3CX's "Automatic Global IP Blacklist" feature, which exchanges data with the 3CX Anti Hacking Defense Program, blocking known suspicious or malicious IPs.

- Blacklisted IPs remain blocked for **31 days** (2,678,400 seconds).
- 2. **Transport Layer Security (TLS)**
 - We only allow **TLS 1.2** for secure SIP (Session Initiation Protocol) connections.
 - We have valid TLS certificates and keys installed, ensuring encrypted call setup and preventing unauthorized access.
- 3. **DoS (Denial of Service) Protection**
 - Each IP is limited to **20 requests within 2 seconds**; exceeding that threshold leads to immediate blacklisting.
 - **Fake or excessive registration attempts** (e.g., 500+) from a single IP are automatically blacklisted.
 - If traffic spikes beyond **1,000 packets in 100 ms**, the IP is temporarily blocked; exceeding **2,000 packets** results in a 31-day block.
- 4. **Geographic Restrictions**
 - We allow calls **only** from North American and European country codes.
- 5. **Authentication Limits**
 - An IP is blacklisted if it has **more than five** failed authentication attempts in 3CX.

These measures provide robust protection against fraudulent or abusive calling practices, helping ensure that any suspicious activity is quickly identified and blocked. Because we make only manual calls and rely on a third-party provider for SIP trunking, the 3CX system does not pose a risk of generating robocalls.

8. Systems in Scope - Robo Call Mitigation

General Overview

Mitigation versus Prevention

Voice service providers and most consumers are familiar with robocall prevention measures to block suspected robocalls at termination. Robocall prevention provides relief to subscribers who are tired of getting nuisance robocalls.

The TRACED Act and subsequent FCC orders require robocall mitigation to prevent robocalls at origination.

Robocall prevention: Reduce or eliminate incoming illegal robocalls while terminating calls to your subscribers.

Robocall mitigation: Reduce or eliminate outbound illegal robocalls originating on your network. The TRACED Act and FCC orders mandate robocall mitigation for calls originating with U.S. NANP numbers.



Robocall Mitigation Methods

Blacklists

You can use blacklists to mitigate robocalls with specific attributes, including:

Calling telephone numbers or prefixes

Calling SPIDs (OCNs) that are not yours

Calling locations, e.g., states/provinces/regions that are not yours

Calling countries that are not yours

IP addresses that you have identified as robocallers

User agents that your customers do not use, but robocallers do use.

When a call is identified by a blacklisted attribute, you can either block the call or divert it to a CAPTCHA gateway for Interactive-Voice-Response screening. You can review blacklisted call origination reports to investigate the underlying causes.

SHIELD

You can use Shield for robocall mitigation to screen calls at origination for calling numbers that are invalid, high-risk, or appear on Do Not Originate lists.

You can set policies by groups, subscribers, and numbers to control the handling of such calls. For example, these calls can be blocked, diverted, or reported.

Shield is a service that identifies high-risk and invalid telephone numbers. The service can inspect inbound calling numbers and/or the outbound called number. By catching these numbers, Shield can quickly prevent unwanted or malicious calls.

Phone Number Reputation Lookup

You can perform a phone number reputation lookup on calling numbers at origination for robocall mitigation. This lookup returns a reputation score from 0 to 100. The higher the number, the worse the reputation.

If your customer has a calling number with a poor reputation, you may find that they are a victim of number spoofing.

Dynamic traffic analysis

You can use real-time dynamic traffic analysis, called SIP Analytics, to detect and mitigate robocalls at origination. SIP Analytics monitors all originated calls by source over a rolling 60-minute window. It compares cumulative call count by source within this window with thresholds that trigger a response to a robocalling event.

SIP Analytics is self-learning. Thresholds are based on call history and are updated dynamically in real time. A legitimate high-volume caller would therefore acquire a higher threshold, while a residential consumer would typically acquire a lower threshold. Default thresholds are used for a new source until it accumulates sufficient history to enable the calculation of dynamic thresholds.

When a cumulative call count for a specific source breaches a threshold, calls from that source can either be blocked or diverted. In either case, you can investigate to determine whether the caller was originating unlawful robocalls.

CAPTCHA

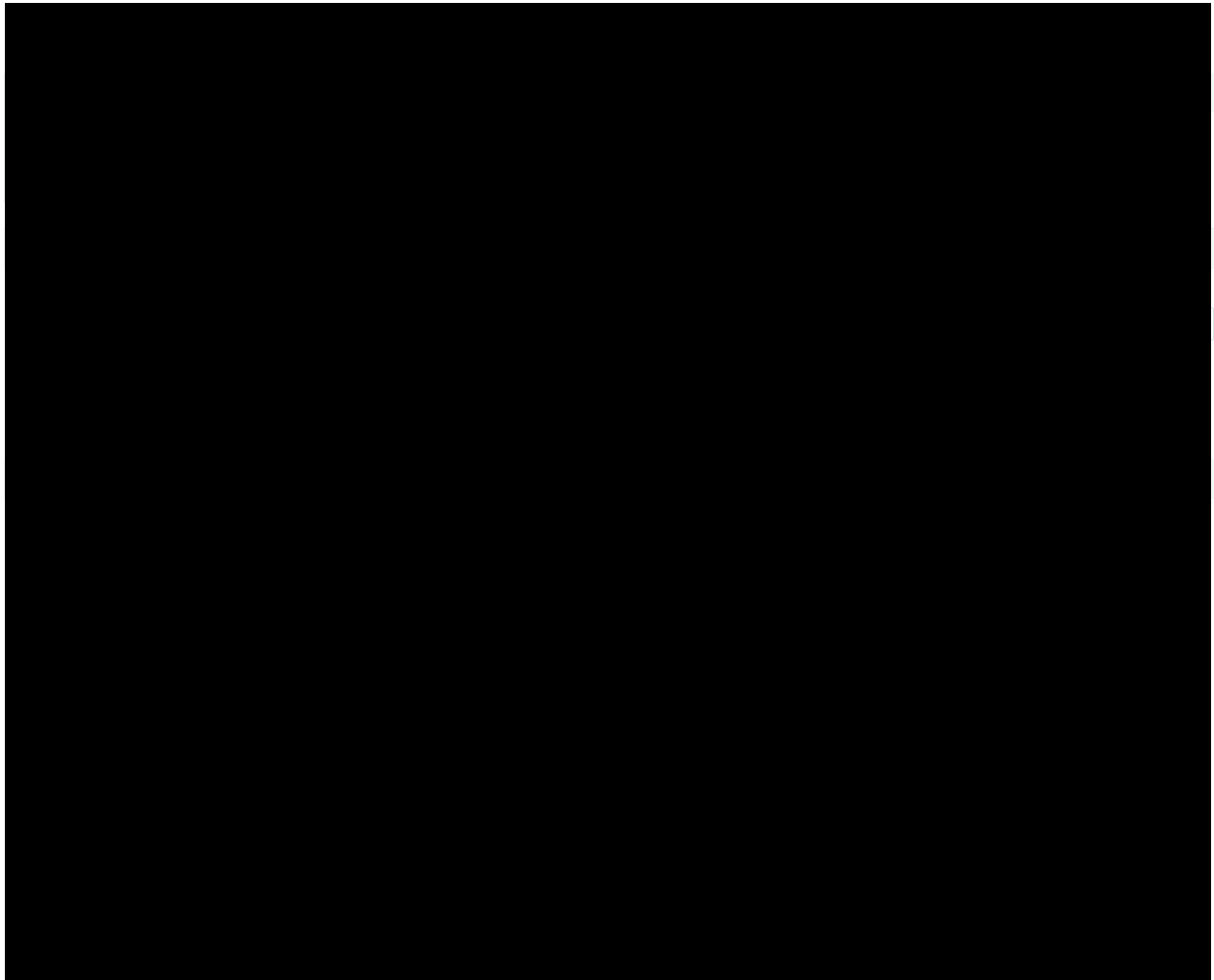
The CAPTCHA gateway can be used in conjunction with the robocall mitigation methods listed above. When a method triggers an action, the CAPTCHA can be invoked to determine whether the caller is a human or an autodialer.

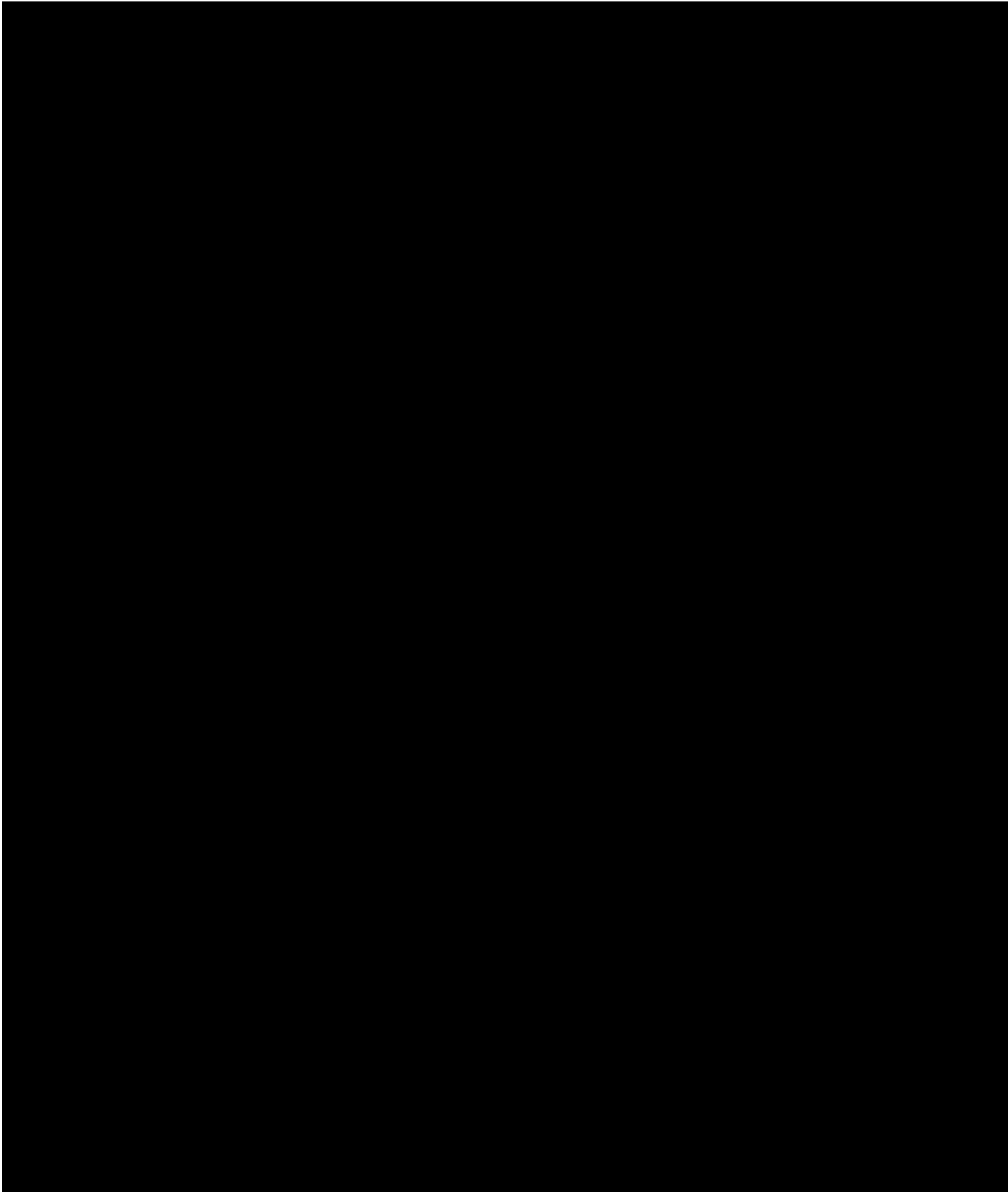
The CAPTCHA prompts the caller for a random two-digit code. If a human is placing the call and they answer the prompt correctly, then the CAPTCHA gateway will allow the call to proceed. If the call is placed by an autodialer, which cannot answer the prompt correctly, then the call can be blocked, diverted to voicemail, or reported.

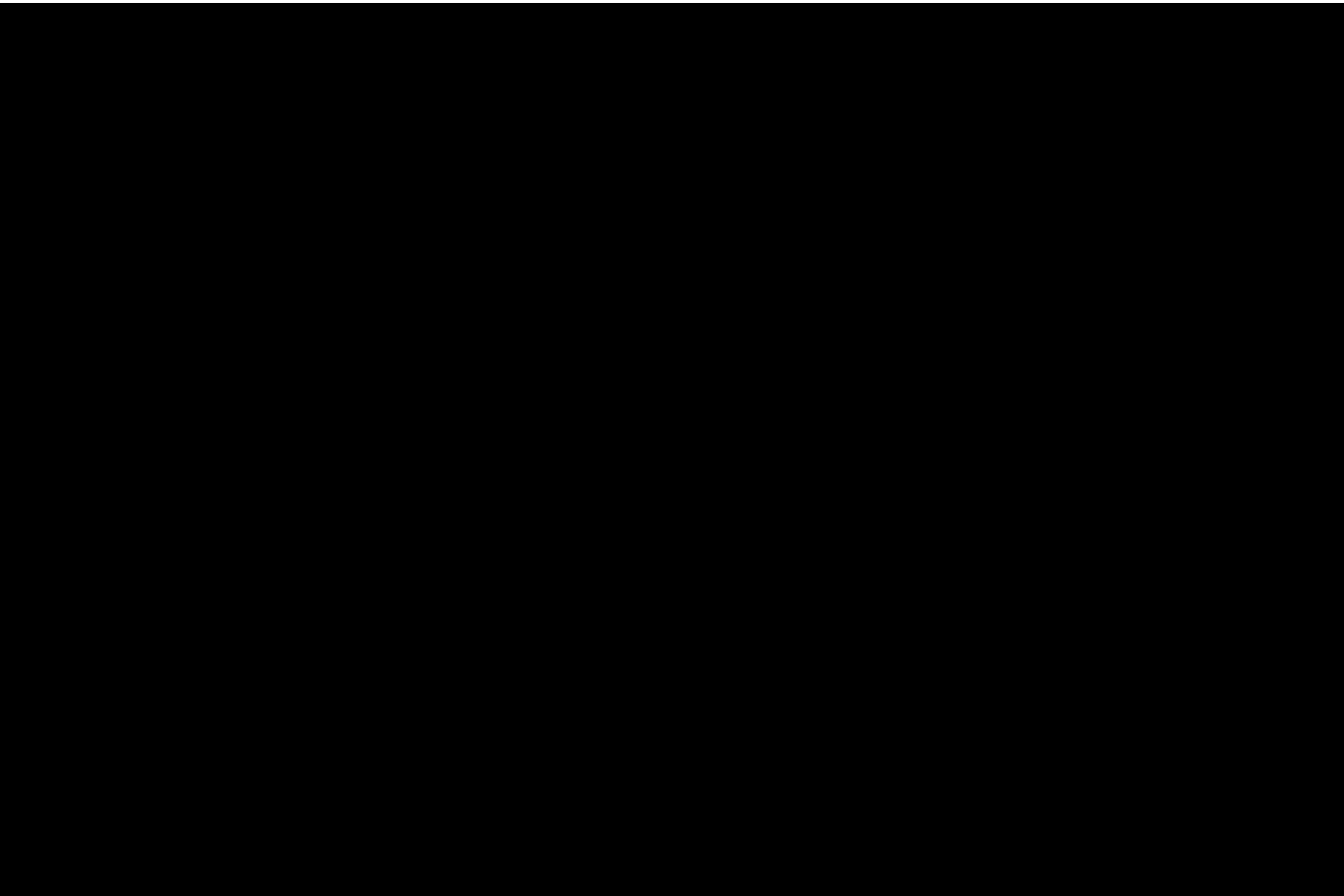
Call Detail Record (CDR) analysis

You can collect CDRs from your network equipment and review them with software such as NexOSS for robocall mitigation. You can develop reports to look for unexpected high call volume, short call duration, call hang-ups by called party, and so forth. If you find suspicious call activity, then you can investigate.

3CX







9. Systems in Scope - Role(s) Provider Plays In The Call Chain

Vix Technology specializes in the development and implementation of Fare Collection Systems for Public Transit Agencies. As part of our contractual obligations for Valley Metro, we utilize third-party services for telephony infrastructure and call center operations.

Specifically:

- Trachmar operates the call center and handles customer interactions on our behalf.
- 3CX provides the hosted phone system that facilitates call routing and management.

- DiD Logic supplies the SIP Trunks that connect the phone system to the public telephone network.

Vix Technology's role in this call center ecosystem is limited to contracting and integrating these services to ensure seamless customer support as part of our Fare Collection System offerings to municipal public transit customers. We do not operate, manage, or directly provide voice services to the public. Vix provides management and oversight to our third party subcontractors and suppliers who support the delivery of the voice service functionalities described herein.

10. Traceback Requests

Vix is committed to ensure that we respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.

Traceback requests can be made to compliance@vixtechnology.com

11. Compliance, Maintenance and Review

This policy is subject to regular, ongoing management review and will be reviewed at least annually or when significant changes to the business occur.

12. Non-Compliance

Failure to comply with any element of this policy may result in disciplinary action, up to and including termination of employment, in accordance with the employee code of conduct and company disciplinary policies..

If you are unsure how to comply with this policy or require any guidance then please contact your local security team via one of the following email addresses:

- security@vixtechnology.com

- security@kubapay.com

13. Acknowledgement

By reading this policy you acknowledge that you have read and understood this document.