

Robocall Mitigation Plan
For Ewart technologies, Inc. dba IsleCall Communications
FRN# 0020756599

Ewart Technologies, Inc. is a small VoIP service provider with less than 100,000 subscribers as defined in §64.6304. We have implemented the following Robocall Mitigation Plan for compliance with the TRACED Act and STIR/SHAKEN.

New Customer Onboarding

Risk Area: Small business and residential voice service customers pose the lowest risk of robocall origination; larger commercial customers and VoIP wholesale customers pose the highest. Many foreign illegal robocallers use VoIP services and DID numbers from the North American Numbering Plan ("NANP") to suggest that their calls were originated within the United States. Customers located outside the United States using NANP numbers require a much deeper investigation before onboarding those customers.

Mitigation: All voice customers are direct customers as we do not provide wholesale or gateway services. We operate only in Florida, and customers are typically known to our organization prior to providing service to them. Nearly all of our customers are small or medium sized businesses, and most are professionals (i.e. Doctor, Lawyer, CPA) or a regulated industry (Financial Services) for which information is readily available to vet the organization.

We do not have on-line signup or automated provisioning of services and personally know all customers who are provided connectivity to our systems. This familiarity makes identifying probable risky customers easy.

Risk Area: VSPs should collect and verify information for each commercial customer such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business. Firmly establishing the existence of the customer can prevent easy spoofing of corporate identity by bad actors.

Mitigation: We typically have existing business relationships with customers directly or indirectly, prior to providing them voice services. Any organization for which we do know have direct knowledge of is researched as part of our onboarding process. This is for risk mitigation in several areas including robocalling, fraud, and credit worthiness. Tools available to vet companies include Sunbiz.org, public databases, social media, references, etc.

Risk Area: Provisions requiring customer assistance in traceback investigations should be included in all service contracts.

Mitigation: Verbiage has been added to our terms and conditions as part of our master service agreement.

Risk Area: The FCC has announced it will create a database of approved entities, the Service Provider Registration Portal, for use by law enforcement, as well as screening by intermediate and terminating voice service providers.

Mitigation: We have a CORES account and are registered with the FCC for inclusion in their database. We have established roles within the organization to ensure that information is kept up to date, and for the purpose of liaison with law enforcement, other carriers, etc.

Ongoing Monitoring and Service

Risk Area: End user customers should have access to call blocking mechanisms that are free and easy to use at the individual number and network level. VSPs should regularly update these systems and communicate with customers to ensure they are aware of the caller ID and blocking mechanisms available to them.

Mitigation: We provide managed services to the majority of our customers. Our [REDACTED] systems have functionality to permit call blocking. Our systems can also provide call blocking for customers with SIP trunks and their own PBX systems. We provide these services without charge to customers.

Risk Area: Dynamic Traffic Analysis can identify behaviors which indicate illegal call activity, such as intermittent bursts of high activity, suspiciously low call completion rates/short call times, and evidence of systematic calling, or “war dialing.” Abnormally high-volume call patterns from a commercial customer is a common symptom of illegal robocalling. Illegal call originators can sometimes be identified by examining Call Detail Records and checking numbers dialed against the National Do Not Call Registry.

Mitigation: Systems are in place to monitor call activity and detect abnormal calling patterns. Monitoring includes call volumes, calls per second, registrations per second, invites per second, high risk destinations, etc. High volume customers are monitored for compliance on a regular basis. All outbound calls are processed by a fraud management system, which also provide STI-PA certification for calls. We proactively block VoIP traffic from high-risk countries and manage access to our systems in a granular manner. Repeated malicious activity or attacks on the system will result in the IPs of the offenders being firewalled.

Risk Area: It may be necessary to contract with third party vendors for these advanced services. VSPs are prohibited from adding a line-item charge for robocall mitigation to customer bills.

Mitigation: Internally, we utilize [REDACTED] to monitor all calls and identify or detect problems. We also utilize the services of [REDACTED] to provide monitoring and fraud detection, STI-PA, and least cost routing for calls. Customers are not charged for these services.

Risk Area: When traffic analysis indicates the presence of likely illegal robocalling, VSPs must have a plan for investigating and addressing the behavior. Responses can include conducting traceback investigations to identify the source of the calls, verifying suspicious activity with customers, suspending customers who are putting robocalls into the system, and contacting relevant law enforcement agencies. VSPs should have a mechanism for halting customers' ability to make new calls and suspending service once illegal robocalling is detected.

Mitigation: The monitoring systems provide alerts to our NOC. If suspicious activity is detected we first investigate it to determine the source and nature of the activity. We will then contact the customer to inquire about the calls and obtain information to determine if these are actually problematic calls. Depending on the severity of the situation, we will restrict calling for the customer as is determined to be appropriate.

Decisions to limit and/or terminate service are made on a case-by-case basis, considering the totality of the circumstances. It is our policy to be aggressive in ensuring our network is not used for malicious or illegal activity. We have zero tolerance for illegal activity on our network.

As part of our ongoing quality assurance and strategic planning, we periodically review our processes and adjust them, if necessary, to address emerging issues.

Response to Illegal Robocalling

Risk Area: Traceback investigations into the origins of illegal calls are a major component of STIR/SHAKEN enforcement and robocall mitigation even for VSPs who have not yet fully implemented STIR/SHAKEN authentication. In addition to conducting their own traceback investigations into suspicious activity, VSPs should be ready to comply with traceback requests by law enforcement, the FCC, or the Industry Traceback Group, the official consortium designated to lead private traceback efforts. Companies should designate a single point of contact to handle traceback requests and coordinate with outside investigations.

Mitigation: The point of contact for investigations and traceback requests is our CEO, who architected and implemented the majority of our systems. Upon receipt of actionable information into our NOC, we will investigate the activity. We have sufficient monitoring in place to positively identify the source of any call that transits our network, and are able to provide this information to an appropriately authorized organization. We anticipate that the majority requests will originate from an involved carrier, the FCC or law enforcement.

Risk Area: It is imperative that VSPs maintain regular contact with state attorneys general in order to stay on the same page as law enforcement and government. As with traceback investigations, companies should have a designated single point of contact for states to reach. The establishment of regular formal channels helps keep both state officials and private actors up to date on the latest robocall mitigation technologies and standards. With the techniques for creating mass robocalls constantly changing, industry wide public-private communication is crucial to keeping networks secure and up to date.

Mitigation: We have reviewed the recommendations of the Attorneys General to the FCC and believe we have implemented appropriate processes and technology to minimize the risk of our network being used for robocalling. Our CEO is a member of and participates in the FBI's Infragard program, which provides resources and information related to critical infrastructure protection. As with other aspects of our plan, the CEO is our designated point of contact with any requests from external parties.