



Epcom Global Networks

Robocall Mitigation Program



Compliance Document Release for Epcom Global Networks:

This packet is prepared for the review and understanding of the obligations of the Robocall Mitigation Program. The Robocall Mitigation Program is an FCC required telecommunication program developed to ensure that all telecommunication providers can detect, block, and report robocall or malicious / SPAM traffic on their networks. Epcom Global Networks – complies with ALL STANDARDS related to this FCC program. This packet will attest and provide our governing policy of the following items:

- Certification of Call Traffic is Subject to Robocall Mitigation
- Detailed Robocall Measures and Practices Along Call Path to Ensure Compliance
- Robocall Mitigation Issues and Traceback Request Support

New York City
Boston – Providence - CT
Washington, D.C.
London, United Kingdom

Website: <http://www.epcomworld.com>
Email: rpancaro@epcomworld.com

Toll Free: 1-877-EPCOM-OK
Phone: 212-203-9278
Fax: 212-203-3219

Table of Contents

Public Release Statement - Introduction	3
Company Summary	4
I. About Robocalls – Certifications of Traffic	5 – 6
II. Robocall Mitigation Program / Plan	7 – 10
III. Traceback and Adherence to FCC Compliance	12
IV. Updates and Final Certifying Information	13

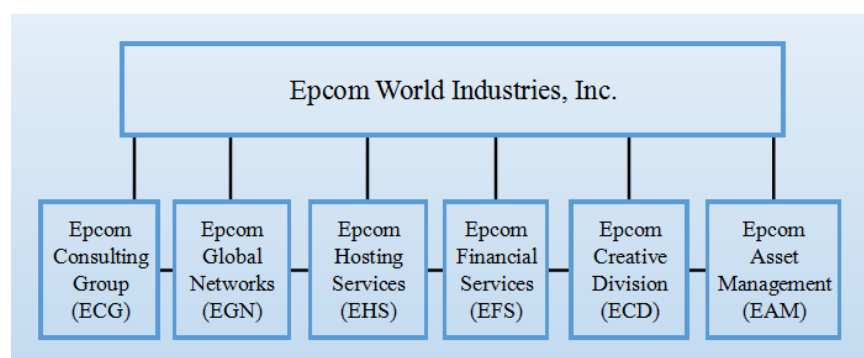
Public Release Statement – Introduction

The information in this Robocall Mitigation Packet is meant for public release. This document complies with the terms of the Federal Communication Commission and definitions set forth under 47 C.F.R § 64.6300. In compliance with the applicable orders and regulations of the Federal Communication Commission this certification packet reviews the operating procedures for Epcom Global Networks a Division of Epcom World Industries, Inc. (a Connecticut Corporation). Epcom Global Networks takes exhaustive measures to prevent unlawful and unauthorized robocalls from originating, terminating, carried, delivered, and processed on the national Epcom Global Networks Telecommunications Platform. Epcom Global Networks is a voice service provider that serves end users, and acts as a reseller, wholesale provider, originating provider, terminating provider, and specialty government emergency telecommunications alerts provider.

Epcom Global Networks DOES NOT carry any non-verified wholesale call center voice traffic. Core clients at Epcom Global Networks are business to business clients such as healthcare (hospital / medical office), education (university), government (local / state / federal), financial institutions (banks / credit unions), and other approved and verified organizations that are then authorized to use the Epcom Global Networks Telecommunications Network. Advanced monitoring of all systems and limited call paths per client prohibit robocall traffic to originate on our platform. Epcom Global Networks terms of services permits the Epcom Global Networks NOC to immediately revoke, block, and suspend traffic classified as potentially suspicious, fraudulent (VoIP Fraud), or robocall related. The Epcom Global Networks team monitors 24 x 7 x 365 all systems and client traffic to ensure the safety and integrity of our platform, but also the larger North American Telecom platforms as a whole.

Company Summary

Epcom World Industries, Inc. provides the greatest products and services in the technology sector for home, home office, business, non-profit, education, and government. At Epcom, everything falls under the Epcom World Industries, Inc. “umbrella / brand”, with all divisions providing unparalleled products and services. The diagram below will help you understand the Corporate Hierarchy of Epcom World Industries, Inc.



*All divisions have a three or four letter group identifier. **Not all divisions listed above.

This Robocall Mitigation Program Document focuses on the Epcom Global Networks (EGN) division of Epcom World Industries, Inc. Epcom Global Networks is the telecom services arm that provides, DID Telephone Numbers, SIP / VoIP phone calls, inbound calling, outbound calling, Fax T.38 Protocol Support, on premise and hosted PBX platforms (integrated only with Epcom Global Networks Telecom Services), SMS Security Transport and Notifications. EGN provides businesses with all the telecom tools they need to safely / securely transact business and stay in touch with their clients. Every client at Epcom Global Networks is verified before being allowed to sign-up (his applies throughout our North American Footprint). No online sign-ups for Epcom Global Networks Telecommunications services – permitting self-provisioning are permitted. Epcom Global Networks knows every client and the type of traffic that is run on our telecom network to ensure all service level agreements are met for our Enterprise Clients.

I. About Robocalls - Certifications of Traffic

Robocalling is defined as a phone call that uses a computerized autodialer to deliver a recorded message or connect the call to a live person. Robocalls can be used for a variety of purposes, including: Political campaigns, Telemarketing, Business Remainders, Public Service Announcements, and Emergency Announcements. Robocalls can be legitimate if they are made to customers who have given consent to receive them. However, robocalls that are used to sell a product or service without prior permission are illegal and are likely scams. Some examples of robocall scams include:

- IRS Scams
- Charity Scams
- Travel Scams
- Health Insurance Calls
- Loan Scams
- Customer Care Scams
- Free Trial Scams
- Auto Warranty Scams

To minimize the risk of being scammed by robocall, you can:

- Hang up as soon as you realize it's a robocall
- Avoid saying "yes" if you can
- Avoid following the bot's instructions

Robocalls can be reported to the Federal Trade Commission at donotcall.gov. You can also register your number with the National Do Not Call Registry.

Epcom Global Networks **certifies** that all traffic originating on our network is subject to the terms of the Robocall Mitigation Program, our prior certification has not been removed or revoked by the Federal Communication Commission, and Epcom Global Networks has not been prohibited from filing in the Robocall Mitigation Database by the Commission (47 C.F.R. § 64.6305(d)(1)). Epcom Global Networks also certifies that the implementation of STIR/SHAKEN across our entire network footprint and all calls originating from our platforms are fully compliant with 47 C.F.R § § 64.6301 (a)(1) and (2).

Based on the Federal Communication Commission Publication of 47 C.F.R § 64.6305(d)(2)(ii) and (iii), Epcom Global Networks – Remote Mitigation Program has been publicly released and shared to the national community reflecting the reasonable steps to avoid originating illegal robocall traffic and includes a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement and the industry traceback consortium. We understand and wish to help aid and support all entities in investigating and stopping any illegal robocallers and use its service to originate calls and abuse phone customers for nefarious purposes.

II. Robocall Mitigation Program / Plan

Epcom Global Networks has developed a list of core measures / requirements in order to ensure the successful performance of all Robocall Mitigation Program requirements as outlined by the Federal Communications Commission – these include:

- A. Knowing your customers
- B. Upstream provider protocol / procedures
- C. Requiring Contractual Documents to Ensure Compliance
- D. Validating Client's Right to Use Utilize a Number – ensuring they are a verified business
- E. Accepting Traffic from Providers in the Robocall Mitigation Database
- F. Monitoring Network Traffic and Network Fraud over Epcom Global Networks – Technology Fabric
- G. React immediately to suspicious calling pattern triggers
- H. Verify International Foreign Providers may not utilize and run traffic over the Epcom Global Networks Technology Infrastructure
- I. Voice Traffic Authentication Procedures – Credential Handling
- J. Employee Training – Continuing Education
- K. Responding to all Federal Communication Commission, Law Enforcement Agencies, and Industry Traceback Requests within 24 Hours if not sooner
- L. Assigning a point of contact for addressing robocall mitigation issues and concerns
- M. Procedures for Updating Epcom Global Networks Submissions and Robocall Mitigation Future Revisions / Documentation Updates

Epcom Global Networks is committed to minimizing the number of robocalls that originate on our network and prevent unwanted robocalls from reaching Epcom Global Networks clients / users. These measures outlined below will help other carriers and the Federal Communications Commission understand the commitment Epcom has to the global telecom community to ensure no abuse occurs on our network by our clients or reaches onto our network from unauthenticated peers / bad actors trying to making fraudulent calls to our clients.

A. Know Your Customer: is an important aspect of knowing the type of entity you are offering services too and understanding the way in which they want to use your service. Epcom Global Networks requires all new and renewing customers to provide and maintain accurate information, including legal name and contact details, and to update and verify this information as needed. Epcom Global Networks uses analytics to help identify suspicious information. As described below, Epcom Global Networks continuously monitors its network for suspicious activity. Epcom Global Networks requires all resellers to institute affirmative, effective measures to know the identify of resellers' clients and their right to use telephone number resources.

Epcom Global Network also requires that all clients fill our Letter of Agency forms, signed by a individual or managing director at a company stating they will comply with the our terms of service for providing that person or organization telecommunication related resources. Epcom then verifies this information even for our reseller partners to make sure only known good entities are allowed to utilize our network resources for their telecom needs. This verification is necessary

to not only ensure the integrity of our network, but also, permits Epcom Global Networks Compliance and Forensic Teams to promptly respond to traceback requests and enforcement efforts.

B. Upstream Provider Protocol Procedures: If the customer is a Voice Service Provider, Gateway Provider, Non-Gateway Intermediate Provider, Foreign Voice Service Provider, and / or Foreign Intermediate Provider, Epcom Global Networks will confirm that the provider is appropriately listed in the Federal Communication Commission Robocall Mitigation Database and has not been delisted pursuant to an enforcement action before accepting traffic from the provider. All Epcom Global Networks providers are US Tier 1 Voice Service Operators and therefore, are compliant with the Robocall Mitigation Program. We work in tandem with our peering partners to ensure that both Voice Operators meet the necessary requirements and aid one another in ensuring easier administration on these protocols / procedures.

Though additional workflows are required to meet the compliance of these various programs, these measures and procedures are effective to prevent new and renewing customers from using our network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring illegal outbound traffic is not run on our platform (47 C.F.R. § 64.1200(n)(3) and know / verify our upstream providers (47 C.F.R § 64.6305(d)(2)(ii).

C. Requiring Contractual Provisions: Normal operations at Epcom Global Networks require clients to be under a contract or service level agreement for services to be provided to them. As such all clients are subject to the Epcom Global Networks – Terms of Service, which includes detailed procedures related to utilizing telecommunication services in a malicious manner, understanding that Epcom Global Networks has the authority at any time and with or without notice to the client to suspend and terminate service, and permit Epcom Global Networks to access client accounts call records and information to investigate complaints or allegations of abuse or unauthorized use of our platform / technology systems with or without notice to the client. Epcom Global Networks has the right under our terms of service to amend our terms of service from time to time without notice, and that the customer is responsible for compliance with the latest revision of the Epcom Global Networks Terms of Service. Revision numbers on all documents are included so tracking can be done from version to version to understand that a new release has been provided.

D. Validating a Client's Right to Use a Number: Upon the request for service by a retail or business subscriber – Epcom Global Networks confirms the end user client has a verified association with the telephone numbers for which they are requesting or originate phone calls. In this connection, Epcom Global Networks either assigned the telephone number to its VoIP end user clients or ports an existing end user's client telephone number on the Epcom Global Networks Platform.

Upon the successful verification of a client's right to use a telephone number, Epcom Global Networks requires a client to submit a signed letter or authorization for right to port of a number, last month of billing from the losing service provider, and any Account Number / PIN information to ensure a smooth and validated port process for not just the team at Epcom Global Networks going to provide the client future service, but also the losing service provider, and end user client requesting the service, etc. This ensures that all parties from the client to the phone operators are confirming and ensuring successful migration of validated services / accounts.

Epcom Global Networks pre-programs all switch fabric that it assigns with only the validated numbers / Caller ID outbound numbers of authorized ports of validated users. Epcom Global Networks clients cannot change this information on their own and any changes must be submitted in writing via our online support platform, undergo re-validation, then the Epcom Global Networks Team will update any validated information. This procedure is the same for any number either ported into the Epcom Global Networks Platform or assigned a new number via the Epcom Global Networks – Number Database Platform. Each client at Epcom Global Networks is assigned a concurrent call path limit and therefore based on what the client is subscribing too cannot run large voice or call center traffic on our network without us knowing about it and validating any such requests in advanced. This type of traffic is NOT generally permitted at Epcom and accounts for less than 1% of total traffic run on our telecom infrastructure. We do not consider our end user clients to be a high risk of originating illegal robocalls or spoofed calls on any Epcom Global Networks Call Path Infrastructure. Regardless, various actions plans are in place to prevent the origination of malicious traffic on our platforms.

E. Epcom Global Networks – will ONLY accept network / voice traffic from providers that have affirmatively filed in the Robocall Mitigation Database: In accordance with the Federal Communication Commission rules:

Accepting traffic from domestic Voice Service Providers: In accordance with 47 C.F.R § 64.6305(g)(1), Epcom Global Networks accepts calls directly from a domestic Voice Service Provider only if their Voice Service Provider’s filing appears in the Robocall Mitigation Database and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Foreign Voice Service Providers or Foreign Intermediate Providers: In accordance with 47 C.F.R § 64.6305(g)(2), Epcom Global Networks accept calls from Foreign Voice Service Providers or Foreign Intermediate Providers that use NANP resources that pertain to the U.S. in the Caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider’s filing appears in the Robocall Mitigation Database and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Gateway Providers: In accordance with 47. C.F.R § 64.6305(g)(3), Epcom Global Networks accepts calls directly from a Gateway Provider only if that Gateway Provider’s filing appear in the Robocall Mitigation Database, shows that the Gateway Provider has affirmatively submitted the filing, and has not been de-listed pursuant to an enforcement action.

Accepting traffic from Non-Gateway Intermediate Providers: In accordance with 47 C.F.R § 64.6305(g)(4) and its effective date, Epcom Global Networks accepts calls directly from a Non-Gateway Intermediate Provider only if that Non-Gateway Intermediate Provider’s filing appear in the Robocall Mitigation Database, shows that the Non-Gateway Intermediate Provider has affirmatively submitted the filing, and has not been de-listed pursuant to an enforcement action.

Epcom Global Networks Know Your Upstream Provider procedure involves checking the Robocall Mitigation Database to see if:

1. The provider’s filing appropriate appears in the Robocall Mitigation Database
2. Shows that the provider has submitted the applicable filing

3. Has not been de-listed pursuant to an enforcement action

All Epcom Global Networks Tier 1 Connecting – Intermediate providers of voice traffic are listed in the Robocall Mitigation Database. Epcom Global Networks does not connect with any other gateway or providers their own current Robocall Mitigation Database Verified Providers and therefore is compliant with all requirements

F. Monitoring Network Traffic and Network Fraud: Epcom Global Networks monitors all technology infrastructure 24 x 7x 365. Our technology NOC team reviews high-volume voice traffic on our network – which could be related to voice fraud or robocall abuse. These incidents are extremely rare if at all occurring on our technology platform. Epcom Global Networks will analyze traffic to identify and monitor patterns consistent with robocalls or other high rate limiting incidents. With the intensive monitoring of voice fraud patterns and protections on our network – this type of call monitoring lends well to similar patterns of Robocall abuse, of which we are able to quickly identify, disable / block, and report on these issues. This is monitored internally by specialized teams at Epcom 24 x 7 x 365 using both in house tools and 3rd party tools to detect and inform our support teams to ensure network quality and integrity at all times.

Should any suspicious activity be found / detected Epcom Global Networks will investigate immediately. Should call traffic be determined to be of fraud or robocall related nature the account will be immediately blocked / suspended / terminated. Should robocalls are illegal or terminating on Epcom Global Networks platform, Epcom Global Networks will work with its Intermediate Providers / Upstream Providers to address and block such traffic.

G. React Immediately to Suspicious Calling Patterns: As noted above – the Epcom Global Networks Security teams are working 24 x 7 x 365 to detect and stop any voice fraud or robocall related issue to keep our network quality and integrity safe and secure. As such our teams are trained to respond immediately to any abuse of our systems. Should Epcom Global Networks detect a pattern consistent with or specific to illegal robocalls (including large bursts of traffic in small timeframes, low duration subscriber traffic and sequential dialing patterns, or calls pattern that is consistent with illegal robocalls), or if it otherwise has good reason to suspect illegal robocalling or illegal spoofing is taking place over its network, Epcom Global Networks will seek to identify the party that is using our network to originate, route, or terminate these calls and take appropriate actions. Such actions Epcom Global Networks takes may include but are no limited to, initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's name, trademark, or DBA name; reviewing complaints; suspending or terminating the party's ability to originate, route, or terminate calls on its network; and notifying law enforcement authorities if need be. Epcom Global Networks Recognizes that foreign originating traffic that uses +1 USA Caller ID Values requires special scrutiny. Epcom Global Networks has procedures in place to monitor foreign inbound domestic United States Traffic Requests and works hard to ensure that no abuse can occur on the North American Dialing Plan Network at Epcom Global Networks.

In the event that Epcom Global Networks determines illegal robocalls are originating on the Epcom Global Networks platform, Epcom Global Networks service to the end user client will be

suspended or terminated in accordance with Epcom Global Networks Terms of Service discussed in several sections above. If the robocalls are illegal and terminating on Epcom Global Networks platform, Epcom Global Network will work with its Intermediate provider to address and block such traffic. To ensure that Epcom Global Networks platform for ourselves, our clients: residential, business, and government, are protected from illegal and potentially fraudulent call traffic, and consistent with contractual limitations and legal considerations, Epcom Global Networks takes these appropriate steps to combat such traffic being originated, terminated, or carried / processed on our platforms as due cause and just.

H. International Providers are NOT authorized to run traffic over the Epcom Global Networks Technology Infrastructure: As part of knowing your customers – Epcom does not permit non-domestic traffic not originating from the country of origin to run against another countries Epcom Global Networks call path platform. Pursuant to 47 C.F.R § 64.1200(n)(5), Epcom Global Networks takes reasonable and effective steps discussed above to ensure that any originating provider or intermediate provider, foreign or domestic, from which it directly receives traffic is not using our infrastructure to process a high volume of illegal traffic onto the United States Network. This is strictly enforced and monitored as outlined by the Epcom Global Networks security teams 24 x 7 x 365. There has never been an incident of International Providers and partner abusing the Epcom Global Networks – United States or North American Infrastructure.

I. Voice Traffic Authenticate Procedures – Credential Handling: Pursuant to 47 C. F.R § 64.6301(a), when operating as a Voice Service Provider, Epcom Global Networks does the following:

- A. Authenticate and verifies caller identification information for all SIP calls that exclusively transit its own network.
- B. Authenticate caller identification information for all SIP calls it originates and that it will exchange with another Voice Service Provider or Intermediate Provider and to the extent technically feasible, transmit that call with authenticated caller identification information to the net Voice Service Provider or Intermediate Provider in the call path.
- C. Verifies caller identification information for all SIP calls it receives which it will terminate and for which the caller identification information has been authenticated.

Credential handling and specific TLS and tokenized voice signaling transport options for clients is also available at Epcom Global Networks. This advanced call signaling and authentication permits clients to have the latest security SIP signaling transport methods as well as provides Epcom Global Networks to benefit from clients wishing to utilize and the latest standards that help us maintain the integrity of our network.

J. Employee Training and Continuing Education: Without proper education and continuing education programs for our staff – Epcom Global Networks – would not be able to provide mission critical 24 x 7 x 365 services and monitoring for our telecommunication platforms. We encourage and support our staff to obtain training and continuing education credits for keeping up and proactively educating themselves on the latest industry threats / risks. Bringing that knowledge back to the company to protect all critical systems at Epcom Global Networks. Based on these trainings and guidance from the Federal Communication Commission our team

stays at the cutting edge of voice fraud and robocall mitigation protection – ensuring the integrity of your call platform and network.

III. Traceback and Adherence to FCC Compliance

K. Responding to all Federal Communication Commission, Law Enforcement Agencies, and Industry Traceback Requests within 24 Hours if Not Sooner: Epcom Global Networks has always been and continues to be committed to fully and timely responding to all such traceback requests from the Commission, law enforcement, and the industry traceback consortium / group (ITG), and will continue to cooperate with such entities in investigating and stopping illegal robocallers that attempt to use Epcom Global Networks Telecommunication Platform. Epcom Global Networks platform is not utilized for the origination, termination, or routing of unwanted and illegal robocalls. In accordance with the FCC's regulations 47 C.F.R. § 64.1200(n)(1) along with 47 C.F.R § 64.6305(a)(2) and (d)(2)(iii), Epcom Global Networks will respond to all traceback requests from the Commission, law enforcement, and the ITG well within 24 hours (this is a 24 hour window applies within business days, per rule 47 C.F.R § 64.1200(n)(1)(ii) and as clarified by the Commission. See also FCC 22-37, at n.211.) and will cooperate with such entities in investigating and stopping any illegal robocallers that attempt to use Epcom Global Networks telecommunication platform and / or services to originate calls. Epcom Global Networks will take the steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau (either via e-mail at compliance@epcomworld.com or via US Mail) and will comply with the requirements of such notice and do so in accordance with the applicable FCC rules (47 C.F.R § 64.1200(n)(2) and (3).

L. Assigning a Point of Contact for addressing Robocall Mitigation Issues and Concerns: Epcom Global Networks is not and has never been utilized for the origination, termination, or carrying or processing of unwanted and illegal robocalls, Epcom Global Networks provides the following name, title, department, business address, telephone number, and e-mail address of the individual within Epcom Global Networks that leads the Epcom Global Networks Team that handles Robocalls Mitigation Related issues – as well as respond to the traceback inquiries from the FCC, ITG, and Law Enforcement Agencies:

Contact Name: Dwayne Edwards
Contact Title: Head of VoIP Transport Services – Epcom Global Networks
Contact Department: VoIP Engineering / Compliance Epcom Global Networks
Contact Street Address: 9 Fairview Drive
Contact City: Pawcatuck
Contact State: Connecticut
Contact Zip Code: 06379-1271
Contact Telephone Number: 212-203-9278
Contact E-Mail: compliance@epcomworld.com

IV. Updates and Final Certifying Information

M. Procedures and Updating of Epcom Global Networks Commission of Robocall Mitigation Database Plan – Final Certifying Information:

Consistent with Federal Communication Commission Regulations, 47 C.F.R. § 64.6305 (d)(5), Epcom Global Networks will update its submission in the Robocall Mitigation Database within 10 business days of any change to the applicable information it must provide and update in the Robocall Mitigation Database.

Epcom Global Networks certifies that all calls that originate on our network are subject to the robocall mitigation program, and prior certification has not been removed by Commission action and they have not been prohibited from filing in the Robocall Mitigation Database.

Epcom Global Networks is not subject to a Federal Communication Commission, law enforcement, or regulatory agency action or investigation due to suspect unlawful robocalling or spoofing.

Epcom Global Networks supports all aspects of 47 C.F.R § 64.6300 and is committed to ensuring the genuine traffic on not just originating from our network, but ensuring the we work with all telecom consortiums to aid in the successful compliant of all robocall mitigation efforts to protect the larger integrity of all North American / Global Telecom Systems / Infrastructure.