

MarketSpark Robocall Mitigation Program – 2026.2

MarketSpark Robocall Mitigation Program Version: February 6, 2026

[Robocall Mitigation Program Introduction](#)

[Company Summary](#)

[Filing of RMP and Implementation of STIR/SHAKEN](#)

[Robocall Mitigation Program](#)

[Implementing Knowing Your Customer Protocols](#)

[Requiring Contractual Provisions to Mitigate Illegal Robocalls](#)

[Only Accepting Traffic from Providers in the RMD](#)

[Blocking Calls on a Do-Not-Originate List](#)

[Analyzing and Monitoring Network Traffic Routing Through MarketSpark's Network](#)

[Ensuring Foreign Providers Are Not Using MarketSpark to Carry or Process High-Volume Illegal Traffic onto the U.S. network](#)

[Authenticating Voice Traffic](#)

[Responding to Commission, Law Enforcement and ITG Traceback Requests](#)

[Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues](#)

[Updating MarketSpark's RMD Submission and RMP](#)

[Business Identifying Information](#)

[Addendum to Robocall Mitigation Program](#)

Robocall Mitigation Program Introduction

MarketSpark offers interconnected VoIP services to its subscribers on a resold basis using the services of IDT Telecom, Inc. While MarketSpark necessarily relies on the robocall mitigation politics, procedures, and safeguards instituted by IDT Telecom, Inc., pursuant to the applicable orders and regulations of the Federal Communications Commission ("FCC" or "Commission"), MarketSpark has adopted the following Robocall Mitigation Program ("RMP") to attempt to prevent unlawful robocalls from originating on, terminating to, or routing through MarketSpark voice networks where it is operating as a Voice Service Provider. Unless defined differently herein, capitalized terms used herein have the same definitions as set forth under 47 C.F.R § 64.6300.

Company Summary

MarketSpark, Inc., a Delaware corporation, is a North American provider of cloud communications and traditional communications services. MarketSpark operates under FCC Registration Number (FRN) 0029814894. Its business services make it easy for companies to connect their traditional POTS-capable equipment, such as alarm panels, elevators, fire systems, to modern, VoIP-based PSTN backhaul.

Filing of RMP and Implementation of STIR/SHAKEN

MarketSpark is exempt from a STIR/SHAKEN implementation obligation. MarketSpark lacks control over the network infrastructure necessary to implement STIR/SHAKEN. See First Caller ID Authentication Report and Order, 35 FCC Rcd at 3241, para. 40; 47 CFR Section 64.6304(b).

Robocall Mitigation Program

This RMP applies to MarketSpark's calling platforms and provides information on MarketSpark's policies and procedures on the following topics that are discussed in turn below which "detail[s] the specific reasonable steps MarketSpark has taken to avoid carrying or processing illegal robocall traffic":

1. Implementing Knowing Your Customer Protocols
2. Requiring Contractual Provisions to Mitigate Illegal Robocalls
3. Only Accepting Traffic from Providers in the RMD
4. Blocking Calls on a Do-Not-Originate List
5. Analyzing and Monitoring Network Traffic Routing Through MarketSpark's Network
6. Ensuring Foreign Providers Are Not Using MarketSpark to Carry or Process High-Volume Illegal Traffic onto the U.S. Network
7. Authenticating Voice Traffic
8. Responding to Commission, Law Enforcement and ITG Traceback Requests
9. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues
10. Updating MarketSpark's RMD Submission and RMP

Implementing Knowing Your Customer Protocols

Consistent with the FCC's Caller ID Authentication Best Practices No. 1

(<https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf>) and 47 C.F.R. § 64.1200(n)(3), MarketSpark vets "the identity of retail and wholesale subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources." In so doing, MarketSpark takes "affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic." (47 C.F.R. § 64.1200(n)(3))

In this regard, MarketSpark has implemented appropriate Know Your Customer ("KYC") protocols when onboarding new or renewing customers. As part of its KYC protocols,

MarketSpark requires any customer to provide sufficient information to ensure its legitimacy. Among other things, MarketSpark generally requires its customers to provide the full legal name of the company, state or country of incorporation, the physical address of its operations, the billing name and address (when different), and the customer contact name and telephone number, and nature of the customer's business. As indicated in Section "Only Accepting Traffic from Providers in the RMD" below, if the company is a Voice Service Provider, Foreign Voice Service Provider, Intermediate Provider, and/or Gateway Provider, MarketSpark confirms, in accordance with currently effective FCC rules, that the company is appropriately listed in the FCC's RMD and has not been delisted pursuant to an enforcement action before accepting traffic from such entities. (See 47 C.F.R. § 64.6305(e)(1)-(3))

Requiring Contractual Provisions to Mitigate Illegal Robocalls

Voice service customers of MarketSpark are subject to robust terms and conditions that (1) obligate customers not to use MarketSpark's services for unlawful purposes; and (2) preserve MarketSpark's right to terminate customers for violations of the law.

MarketSpark's contracts include terms that forbid the customer from using MarketSpark's services to originate and/or otherwise transmit calls that violate laws restricting robocalls or other telemarketing calls, including the federal Telephone Consumer Protection Act ("TCPA") and/or the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act ("TRACED Act") and/or the rules promulgated pursuant to these statutes. MarketSpark's contract terms provide that if any calls originated or otherwise transmitted by the customer to MarketSpark violate the TCPA, the TRACED Act, or the rules promulgated under these statutes, then MarketSpark may, at its sole discretion, suspend or terminate the customer's service immediately, among other remedies.

Only Accepting Traffic from Providers in the RMD

As a provider of end-customer services, MarketSpark does not carry traffic for other domestic Voice Service Providers, Foreign Voice Service Providers, Foreign Intermediate Providers or Gateway Providers. As a reseller, MarketSpark necessarily relies on IDT Telecom, Inc. for compliance with the FCC's requirements related to acceptance of traffic. MarketSpark's upstream provider, IDT Telecom, Inc., is registered in the FCC's Robocall Mitigation Database and has described its "know your upstream provider" protocols in its mitigation plan, including assuring that if the company is a Voice Service Provider, Foreign Voice Service Provider, Intermediate Provider, and/or Gateway Provider, IDT Telecom, Inc. confirms, in accordance with currently effective FCC rules, that the company is appropriately listed in the FCC's RMD and has not been delisted pursuant to an enforcement action before accepting traffic from such entities.

Blocking Calls on a Do-Not-Originate List

In accordance with FCC Rules, 47 C.F.R. § 64.1200(k)(2) and (o)(1)-(4), MarketSpark's upstream provider IDT Telecom Inc.'s robocall mitigation plan on file with the FCC reports that it blocks calls purporting to originate from a number on a reasonable Do-Not-Originate ("DNO") list that is associated with North American Numbering Plan numbers, and that it has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number.

Analyzing and Monitoring Network Traffic Routing Through MarketSpark's Network

As a reseller, MarketSpark necessarily relies on its wholesale provider IDT Telecom, Inc. to monitor and detect patterns indicative of potential unlawful robocall and to block such calls. Consistent with Principal No. 5 of the FCC's Caller ID Authentication Best Practices, IDT Telecom, Inc. reports that it monitors voice traffic patterns on a twenty-four (24) hour basis to identify behaviors that are consistent with illegal robocalling and:

- has in place anti-fraud processes that enable it to, among other things, monitor network usage, identify suspicious network activity (based on call duration, abnormal call patterns, atypical call activity, and subscriber information), receive automatic alerts, investigate traffic to distinguish fraud from honest customer usage, and resolve cases intelligently on a case-by-case basis;
- uses internally developed electronic as well as manual customer analytics tools designed to monitor traffic for suspicious patterns (IDT Telecom, Inc. describes that what makes a pattern "suspicious" is the result of multiple factors, which may (and likely will) vary based on numerous considerations including, but not limited to: commercial history with IDT Telecom, Inc. of entity transmitting traffic to IDT Telecom, Inc.; terminating location of traffic; length of calls; originating ANIs of traffic; prior understanding of IDT Telecom, Inc. regarding the traffic to be transported; country/region of originating calls; as well as other factors which may or may not be considered in all instances);
- uses You Mail Protective Services and compares ANIs against a Do Not Originate list provided by Somos, Inc. through their subsidiary, XConnect, to block such traffic automatically; and
- blocks all numbers on the Industry Traceback Group Do Not Origin List and is consistently reviewing and considering the implementation of additional DNO lists.

If MarketSpark receives a report from IDT Telecom, Inc. of suspected unlawful robocall traffic originated by its end-user customer, MarketSpark will investigate. To the extent a customer is found to have violated its terms of service, MarketSpark takes appropriate action to address

such behaviors, which may include working with the originating customer to resolve problematic traffic, blocking the problematic calls and/or terminating the customer's service.

Ensuring Foreign Providers Are Not Using MarketSpark to Carry or Process High-Volume Illegal Traffic onto the U.S. network

As a provider of end-customer services, MarketSpark does not carry traffic for other domestic Voice Service Providers, Foreign Voice Service Providers, Foreign Intermediate Providers or Gateway Providers.

Authenticating Voice Traffic

As a reseller, MarketSpark necessarily relies on its wholesale provider IDT Telecom, Inc. to 1) authenticate and verify caller identification information for all SIP calls that exclusively transit its own network; (2) 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 next Voice Service Provider or Intermediate Provider in the call path; and (3) verify caller identification information for all SIP calls it receives from another Voice Service Provider or Intermediate Provider which it will terminate and for which the caller identification information has been authenticated. (47 C.F.R. § 64.6301(a))

Responding to Commission, Law Enforcement and ITG Traceback Requests

MarketSpark is committed to ensuring that its network 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. § 64.6305(b)(2) and 47 C.F.R. § 64.1200(n)(1)(ii), MarketSpark will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium ("ITG") within-24 hours (This 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 FCC 22-37, at n.211) and will cooperate with such entities in investigating and stopping any illegal robocallers that attempt to use MarketSpark's network to carry or process calls. MarketSpark is also committed to cooperating with IDT Telecom, Inc. regarding any traceback requests received by IDT Telecom, Inc. that are associated with MarketSpark end-user customers. As part of this commitment, MarketSpark will take the necessary steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau and will comply with the requirements of such notice and do so in accordance with the applicable FCC rules. (See 47 C.F.R. § 64.1200(n)(2), (3) & (5)).

Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure MarketSpark's network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, MarketSpark provides the following name, title, department, business address, and email address of the individual within MarketSpark that leads MarketSpark's team that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name: Patrick Burns

Contact Title: Chief Operating Officer

Contact City: Bannockburn

Contact State and Zip Code: Illinois 60015

Contact Email: patrick@marketspark.com

Updating MarketSpark's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), MarketSpark will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its RMP.

Business Identifying Information

MarketSpark, Inc., is a Delaware Corporation. Its headquarters are at 2201 Waukegan Road #140, Bannockburn, IL 60015.

Jeff Gower

Chief Executive Officer

Patrick Burns

Chief Operating Officer

Charlie Wilson

Chief Technical Officer

Addendum to Robocall Mitigation Program

MarketSpark, Sub, Inc. ("MarketSpark"), hereby provides this Addendum to Robocall Mitigation Plan ("Addendum") to MarketSpark's Robocall Mitigation Plan "RMP" (If any statements or other information in the Addendum are in any way inconsistent with statements in the original RMP, the statements in the Addendum shall supersede the previously drafted statements.) in accordance with the obligations set forth in In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Notice of Proposed Rulemaking, WC Docket No. 17-97 (March 17,

2023) ¶¶ 36-52 (“Sixth R&O”). The Addendum shall heretofore be incorporated within and be a part of MarketSpark’s RMP.

In the Sixth R&O, the Commission stated, “First, to increase transparency for the industry and regulators and better facilitate our evaluation of the mitigation plans detailed in the Robocall Mitigation Database, we require providers to submit additional information to indicate the role or roles they are playing in the call chain.” (*Sixth R&O* at ¶ 44) Accordingly, MarketSpark hereby states that for each call it handles that is subject to the Commission’s STIR/SHAKEN rules, MarketSpark is:

1. exempt from a STIR/SHAKEN implementation obligation as it lacks control over the network infrastructure necessary to implement STIR/SHAKEN. Rather, this control and infrastructure is operated by IDT Telecom, Inc., from whom MarketSpark resells services.

In the Sixth R&O, the Commission stated, “Second ... providers with a current Robocall Mitigation Database filing obligation must state in their mitigation plan whether a STIR/SHAKEN extension applies.” (*Id.* at ¶ 45) IDT Telecom, Inc. has implemented its STIR/SHAKEN obligations and has filed its initial RMP and herein MarketSpark files the additional information required by the *Sixth R&O*. Accordingly, MarketSpark hereby states that a STIR/SHAKEN extension is neither requested nor needed and a request for an extension does not apply.

In the *Sixth R&O*, the Commission stated, “Third, we require new and existing filers to certify that they have not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, including the new enforcement requirements adopted herein.” (*Id.* at ¶ 46)

Accordingly, MarketSpark hereby states that it has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, including the new enforcement requirements adopted herein. Moreover, MarketSpark certifies that it has not been barred from filing in the Robocall Mitigation Database by such an enforcement action, including, but not limited to, instances in which a provider has been removed from the Robocall Mitigation Database and has been precluded from refiling unless and until certain deficiencies have been cured and those in which a provider’s authorization to file has been revoked due to continued violations of the Commission’s robocall mitigation rules.

In the *Sixth R&O*, the Commission stated, “Fourth, we require all providers to: (1) state whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging,

assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so (2) provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.” (*Id.* at ¶ 47)

However, the Commission narrowed the possible scope of the reporting obligation when it stated, “We limit this reporting requirement to formal actions and investigations that have been commenced or issued pursuant to a written notice or other instrument containing findings by the law enforcement or regulatory agency that the filing entity has or is suspected of the illegal activities itemized above, including, but not limited to, notices of apparent liability, forfeiture orders, state or federal civil lawsuits or criminal indictments, and inquiries from law enforcement or regulatory agencies or investigations that do not include findings of actual or suspected wrongdoing. Thus, for example, traceback requests, Enforcement Bureau letters of inquiry or subpoenas, or investigative demand letters or subpoenas issued by regulatory agencies or law enforcement would not trigger this obligation because they are not accompanied by findings of actual or suspected wrongdoing. We find that inquiries or investigations that do not contain findings of actual or suspected wrongdoing by the law enforcement or regulatory agency would be of limited value to the Commission in evaluating the certifications and robocall mitigation plans submitted to the Robocall Mitigation Database.” (*Id.* (Footnotes omitted.))

Accordingly, MarketSpark hereby states that it has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description. While MarketSpark has received some or all of the requests listed by the Commission (e.g., inquiries from law enforcement or regulatory agencies or investigations such as traceback requests, Enforcement Bureau letters of inquiry or subpoenas, or investigative demand letters or subpoenas issued by regulatory agencies or law enforcement), these requests did not include findings of actual or suspected wrongdoing. As a result, they do not trigger the aforementioned reporting obligation because they were not accompanied by findings of actual or suspected wrongdoing.

The *Sixth R&O* also requires filers to “submit their OCN if they have one.” (*Id.* at ¶ 48)
MarketSpark does not hold an OCN.

Additionally, in the *Sixth R&O*, the Commission stated, “Specifically, as part of their obligation to ‘describe with particularity’ their robocall mitigation techniques, (1) voice service providers must

describe how they are meeting their existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls; (2) non-gateway intermediate providers and voice service providers must, like gateway providers, describe any “know-your-upstream provider” procedures in place designed to mitigate illegal robocalls; and (3) all providers must describe any call analytics systems they use to identify and block illegal traffic, including whether they use a third-party vendor or vendors and the name of the vendor(s).

In the “Robocall Mitigation Program” Section of its RMP, MarketSpark describes in considerable detail how it is meeting its obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls. That Section is incorporated by reference.

MarketSpark has also, over time, developed contract language to reflect its obligations under current and developing STIR/SHAKEN rules. Below, we have included sample contract language that MarketSpark has developed contemporaneously with the filing of this Addendum. It is not the position of MarketSpark that this language is in all previously signed contracts. Rather, this language is consistent with language presented to new customers, to the degree applicable.

Prohibited Uses. Notwithstanding anything to the contrary contained herein, MarketSpark reserves the right, in its sole discretion, to immediately and without notice terminate the Services to Customer (and generally) for any of the Services or any other action that causes a disruption in MarketSpark’s network integrity, or directly or indirectly threatens or compromises the security of MarketSpark, its vendors, or the Services, or that otherwise violates this Section 6. Permitted use of the Services does not include certain activities including, but not limited to autodialing, robocalling, transmitting any material that contains viruses, time bombs, trojan horses, worms, malware, spyware, or any other program that may be harmful or dangerous, spoofing, continuous or extensive call forwarding, continuous connectivity, fax broadcast, fax blasting, polling, transmitting any material that may infringe, misappropriate, or otherwise violate the foreign or domestic intellectual property rights or other rights of third parties, telemarketing (including without limitation charitable or political solicitation, junk faxing fax spamming, calling/faxing any person through the use of distribution lists or otherwise who has not given specific permission to be included in such a process, or any other activity that would be inconsistent with reasonable business usage. Customer shall not transmit through the Services any unlawful, harassing, defamatory, abusive, threatening, harmful, vulgar, obscene, indecent, or otherwise objectionable communications or material of any kind or nature. Customer further agrees not to transmit any material that encourages conduct that could constitute a criminal offense, violate the intellectual property rights of others, give rise to civil or criminal liability or otherwise violate any applicable local, state, national or international statute, regulation, or other law. Customer

agrees they will, at all times, comply with all applicable law. Applicable law includes, as applicable, the Telephone Consumer Protection Act and the Telemarketing Sales Rule, the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”), the Truth in Caller ID Act, the Junk Fax Act, the CAN-SPAM Act, similar state laws, state laws regarding privacy and data subject rights, and the requirements of the Payment Card Industry Data Security Standard (“PCI DSS”).

Customer warrants and represents that: (1) Customer is not a provider of ‘voice service’ as defined by 47 CFR Section 64.6300(n); (2) Customer is not a ‘foreign voice service provider,’ as defined by 47 CFR Section 64.6300(c); (3) Customer is not an Intermediate Service Provider (ISP), as that term is defined by 47 CFR Section 64.6300(g); (4) all traffic sent by Customer to MarketSpark shall be originated in the conduct of Customer’s legitimate business, on Customer’s equipment, and using originating numbers that Customer has the legal right to use; and (5) neither Customer nor any of Customer’s affiliates or principals have ever been the recipient of a cease and desist, mandatory blocking, or similar order from the FCC, FTC, or other federal or state agency with respect to the transmission of voice or fax traffic. Customer will not send to MarketSpark traffic as a voice service provider, a foreign voice service provider or intermediate service provider (meaning, traffic originated by third parties and transited by Customer).

If any calls originated or otherwise transmitted by Customer to MarketSpark violate the terms of applicable law, then MarketSpark may, in its sole discretion, in addition to the remedies contained in these Terms of Service, suspend or terminate the Services immediately and freeze some and/or all prepaid monies remitted by Customer to MarketSpark until such time that MarketSpark, at its sole discretion, has determined it shall not be subject to any penalties, fines and/or “voluntary contributions” by the Federal Communications Commission and/or other third parties who have or may obtain a legal right of payment. Should MarketSpark be subject to any penalties, fines and/or “voluntary contributions,” MarketSpark may use any frozen payments as partial payment to the third party(ies) and MarketSpark may seek payment from Customer for any additional, required payments. Customer will cooperate with and promptly provide information requested in connection with any traceback requests. Any use found to be inconsistent with any of the restrictions set forth herein may result in the immediate termination of the Services. Customer also understands that MarketSpark may immediately suspend or terminate Customer’s right to use the Services, without liability of any kind, if (a) in MarketSpark’s sole discretion, Customer’s use of the Services exceeds what would be expected of normal business use. MarketSpark reserves the right, in its sole discretion, to block access to certain high cost/premium locations.

Also, as stated earlier in this Addendum, MarketSpark is a voice service provider; a non-gateway intermediate provider and/or a non-gateway intermediate provider. As a result, MarketSpark has “know-your-upstream provider” procedures in place designed to mitigate illegal robocalls. These procedures are as follows.

Consistent with the FCC’s Caller ID Authentication Best Practices No. 1 (<https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf>) and 47 C.F.R. § 64.1200(n)(3), MarketSpark vets “the identity of retail and wholesale subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources.” (*Id.*) In so doing, MarketSpark takes “affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.” (47 C.F.R. § 64.1200(n)(3))

In this regard, MarketSpark has implemented appropriate Know Your Customer (“KYC”) protocols when onboarding new or renewing customers. As part of its KYC protocols, MarketSpark requires any customer to provide sufficient information to ensure its legitimacy. Among other things, MarketSpark generally requires its customers to provide the full legal name of the company, state or country of incorporation, the physical address of its operations, the billing name and address (when different), and the customer contact name and telephone number, the industry in which the customer participates and nature of the customer’s business as well as the customer’s traceback history. If the company is a Voice Service Provider, Foreign Voice Service Provider, Intermediate Provider, and/or Gateway Provider, MarketSpark confirms, in accordance with currently effective FCC rules, that the company is appropriately listed in the FCC’s RMD and has not been delisted pursuant to an enforcement action before accepting traffic from such entities. (*See*, 47 C.F.R. § 64.6305(e)(1)-(3))

Finally, In the *Sixth R&O*, the Commission demands that “all providers must describe any call analytics systems they use to identify and block illegal traffic, including whether they use a third-party vendor or vendors and the name of the vendor(s).” Therefore, as requested by the Commission, MarketSpark, a reseller of IDT Telecom, Inc., hereby describes how IDT Telecom, Inc. is meeting its afore-stated obligations. IDT Telecom, Inc. uses internally developed electronic as well as manual customer analytics tools designed to monitor their traffic for suspicious patterns. IDT Telecom, Inc. considers these tools confidential and proprietary but will make them available to the Commission upon request. What makes a pattern “suspicious” is the result of multiple factors, which may (and likely will) vary based on numerous considerations including, but not limited to: commercial history with IDT Telecom, Inc. of entity transmitting

traffic to IDT Telecom, Inc.; terminating location of traffic; length of calls; originating ANIs of traffic; prior understanding of IDT Telecom, Inc. regarding the traffic to be transported; country/region of originating calls; as well as other factors which may or may not be considered in all instances.

Also, IDT Telecom, Inc. subscribes to/use You Mail Protective Services; IDT Telecom, Inc. compare ANIs against a Do Not Originate list provided by Somos, Inc. through their subsidiary, XConnect, to block such traffic automatically and IDT Telecom, Inc. blocks all numbers on the Industry Traceback Group Do Not Origin List. IDT Telecom, Inc. is consistently reviewing and considering the implementation of additional DNO lists and anticipates adding these Lists as warranted.