



Hinson Communications Inc dba Lines Plus
1314 Ross Clark Circle
Dothan, AL 36301

Robocall Mitigation Compliance with Traced Act

This Robocall mitigation plan of Hinson Communications Inc. ("The Provider") has been prepared in compliance with robocall regulations on <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf> and <https://www.federalregister.gov/documents/2023/06/21/2023-12142/call-authentication-trust-anchor>.

The Provider, nor any of its executives or principals are subject to an FCC, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing and information concerning any such actions or investigations.

(I). Status of STIR/SHAKEN Implementation

The Provider has two upstream providers from which it receives voice services by PayG LLC dba SkySwitch ("SkySwitch") and Coredial ("Coredial"). The Provider has confirmed that PayG LLC has fully implemented STIR/SHAKEN protocols across their VoIP platform and networks (RMD0002940).

1. PayG LLC dba SkySwitch
Arborcrest 1, 751 Arbor Way
Suite 150
Blue Bell, PA 19422
Phone: 747-777-8100
Email: support@skyswitch.com
2. PayG LLC dba Coredial
Arborcrest 1, 751 Arbor Way
Suite 150
Blue Bell, PA 19422
Phone: 215.297.4400
Email: cdsupport@skyswitch.com

The provider has verified with PayG LLC that it complies with 64.6301 Caller ID authentication requirements and other parts of the FCC Robocall regulations. Such as those listed on <https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-HH> and does so by:

- (1) Authenticating and verifying caller identification information for all SIP calls that exclusively transit its own network;
- (2) Authenticating 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, transmits that call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path; and

(3) Verifying 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.

(II). Robocall Mitigation Program

The Provider uses software provided by PayG LLC to monitor its outbound voice traffic to prevent the origination of illegal robocalls. The software provides detailed reporting to identify suspected illegal robocalls and alert the Provider if it originates any calls where the calling number is invalid, unallocated. If the Provider determines that the caller was attempting to originate unlawful robocalls, then it can either warn them to stop or terminate their services as appropriate. Combining behavioral analytics, caller authentication and verification, the solution features:

- (1) Fraud Detection: Detection of high volume robocalling, spoofing and spam call activity.
- (2) Subscriber Notification: Caller ID Name override to warn subscribers of suspicious calls.
- (3) Call Blocking Support: Accurate identification enabling you to blocked fraudulent phone calls as per the TRACED ACT (2019).
- (4) Business Number Verification: Register legitimate business numbers to prevent unintentional call blocking.
- (5) Caller ID Name Service: Easy integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.

(III). Know Your Customer

For each call, the Provider determines the nature of the business of each of its customers, to ensure that its customer do not provide service to those engaged in robocalling. Traffic from the Provider's customers is monitored continuously for patterns of known abuse. Immediate action is taken in situations where it is deemed necessary to prevent robocalling or other forms of fraud. The Provider also uses via PayG LLC data systems for analytics and reviews to identify illegal robocalling in addition to the Know Your Customer (KYC) requirement to access the Company's networks. The process includes:

- (1) Monitoring the network to identify suspicious traffic patterns.
- (2) Limiting Customers capacity via call per second and/or concurrent session limits.
- (3) Regularly checking call patterns for possible abusive traffic.
- (4) All new customers are verified with a combination of electronic and manual verification systems, credit reviews, references from trusted industry members, and previous experiences with customer executives and employees. The company severely limits the capabilities of new accounts until these appropriate processes are complete.

(IV). Traceback

The Provider responds to all traceback requests from the Federal Communications Commission, law enforcement, and the registered traceback consortium and cooperates with such entities in investigating and stopping illegal robocalls that attempt to use the systems of the Provider. When notified by the FFC's Enforcement Bureau, The Provider, shall block and report identified illegal traffic, and any substantially similar traffic (unless the Provider's investigation determines that the traffic is not illegal). In that event, The Provider will submit an explanation as to why it concluded as such.

(V). Know Your Upstream Provider

The Provider has an Upstream Provider Policy required to access the Company's networks to ensure that such customers and providers do not or are not likely to engage in any prohibited conduct. If the customer is a Voice Service Provider, The Company confirms that the provider is appropriately listed in the FCC's RMD and has not been delisted pursuant to an enforcement action before accepting traffic from the provider.