

# **SIK TECHNOLOGY, DBA SERVERSIM**

## **Robocall Mitigation Plan**

The following policies apply to all customers and/or prospective customers of SIK Technology, DBA ServerSIM and comprise our Robocall Mitigation Plan to avoid originating illegal robocall traffic from our network:

1. **CONTRACT REQUIREMENT:** Our agreements clearly prohibit passing illegal robocalls through any of our switches or networks and define precise requirements for ASR, LCD and other traffic statistics. Customers who violate these rules are subject to immediate termination without notification. If SIK TECHNOLOGY, DBA SERVERSIM believes illegal traffic has been passed through its network, the customer sending such traffic forfeits confidentiality and all data will be shared with industry partners and law enforcement as required by regulatory bodies.
2. **CUSTOMER DISCLOSURES AND CONFIRMATION:** All customers are required to disclose certain information about their business such as physical location, contact personnel, state/country of incorporation or business formation, federal tax I.D. or non-USA government I.D. They must also disclose the practices and nature of their business. We endeavor to know the precise type of traffic which originates from each customer's switch, including the type of customers they acquire and exact type of services they provide. SIK TECHNOLOGY, DBA SERVERSIM investigates each Customer's claims to verify accuracy before accepting them as a customer.
3. **MONITORING AND TRACEBACK:** SIK TECHNOLOGY, DBA SERVERSIM monitors its system diligently and will investigate any suspicious traffic. We act promptly when we detect traffic which appears to be robocall activity to ensure it has been preauthorized as "legal" (i.e. authorized political, non-profit, reverse 911 or fully-opted-in traffic). In the event SIK TECHNOLOGY, DBA SERVERSIM receives a Traceback request for an illegal robocall, we act on it immediately, request a specific and detailed explanation from our customer(s) and insist on immediate corrective action. We respond to all Traceback requests from authorities. If corrective action is not timely provided by our customer, SIK TECHNOLOGY, DBA SERVERSIM takes whatever action is necessary to prevent recurrence of the event(s).
4. **PUBLICATION AND NOTIFICATION:** SIK TECHNOLOGY, DBA SERVERSIM publishes in the public section of its website this Robocall Mitigation Plan and further proactively notifies all customers of such policy along with keeping a record of such notifications.
5. **FOREIGN SOURCES OF TRAFFIC:** SIK TECHNOLOGY, DBA SERVERSIM has non-USA customers which service their own customers and traffic that originates from both USA and Non-USA sources. We take extra precautions relative to Non-USA customers to ensure they meet all requirements of this Robocall Mitigation Plan. Prior to authorizing a foreign customer for calling privileges, we verify all information requested.
6. **ROBOCALL MITIGATION DATABASE:** No later than August 30, 2021, SIK Technology, DBA ServerSIM, will require all its wholesale customers to be registered with the Robocall Mitigation Database. Those wholesale customers not registered with this database will not be allowed access to our network.
7. **CALL BLOCKING:** SIK TECHNOLOGY, DBA SERVERSIM blocks all calls originating from numbers known to us to send illegal robocall traffic and/or calls destined to specific phone numbers as appropriate for robocall mitigation.
8. **LAW ENFORCEMENT COOPERATION:** SIK TECHNOLOGY, DBA SERVERSIM cooperates fully with investigative authorities, industry traceback groups, the FCC and the official consortium designated to lead private traceback efforts. We have a single contact individual designated to handle all traceback requests and coordinate with outside investigations.