

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Swift Mobile Solutions LTD, trading as Swifcom
FCC Registration Number: 0033121138
Version 1.0 | Effective 10 September 2026

Filing entity	Swift Mobile Solutions LTD (Swifcom)
Existing RMD record	RMD0012647
Provider status	Foreign voice service provider; voice service provider filing
Current STIR/SHAKEN status	No implementation on any portion of Swifcom's network
Program owner	Chief Technology Officer / officer identified in the RMD filing
Business address	Suite 6, The Belmont, 89 Middleton Road, Manchester M8 4JY, United Kingdom

1. Purpose and scope

Swift Mobile Solutions LTD ("Swift Mobile Solutions" or "Swifcom") maintains this program to prevent its network and services from being used to originate illegal robocalls, to detect and stop suspected abuse promptly, and to support traceback and law-enforcement investigations. The program applies to calls originated through Swifcom-controlled applications, accounts, APIs, SIP access, routing, and carrier interconnections, including calls using U.S. North American Numbering Plan (NANP) caller identification.

All calls originated through Swifcom are subject to this program. The controls are risk-based and combine customer and provider diligence, caller-ID authorization, authenticated access, call-data monitoring, human review, blocking and suspension, record preservation, and cooperation with the FCC, law enforcement, the Industry Traceback Group, and contracted carriers.

This program is intended to satisfy the current requirements of 47 CFR 64.6305(a) and (d), including the specific-plan, know-your-customer, analytics, and 24-hour traceback elements, and the originating-provider obligations in 47 CFR 64.1200(n)(4) and (o).

2. Service and network context

Swifcom is a United Kingdom-based, multi-tenant communications platform. It supplies applications and communications functions including calling, telephone numbers, routing, PBX functions, SIP connectivity, APIs, and carrier interconnection. It may support direct end-user services and separately configured operator tenants. Each account and tenant is logically associated with identified users, administrators, services, numbers, access credentials, routing rules, and billing records.

Swifcom is a foreign voice service provider. It provides voice service outside the United States and can originate calls that terminate in the United States. It therefore files in the RMD so that U.S. providers may accept calls using U.S. NANP caller ID directly from it. Swifcom has not yet implemented STIR/SHAKEN using its own SPC token and certificate and does not claim that a downstream carrier's signing constitutes Swifcom implementation.

3. Know-your-customer and account controls

Swifcom takes affirmative, effective measures intended to prevent new and renewing customers from using its services to originate illegal calls.

- Account identity. Direct users are associated with verified email and/or telephone identity. Business and operator accounts are associated with an identified organization, an accountable administrator, working contact information, and the stated service use case.
- Risk-based review. Before enabling higher-risk calling capabilities, SIP trunks, API access, multiple numbers, elevated channel capacity, or unusual destinations or volumes, Swifcom may request and review additional business, ownership, address, website, payment, anticipated-traffic, and authorization information.
- No anonymous unlimited origination. Calling access is tied to an authenticated account or tenant. Consumer usage is pay as you go from an account wallet; SIP capacity is provisioned by channel. These controls create accountable service boundaries and limit unapproved scale.
- Renewal and change review. Material account changes, requests for additional capacity or caller IDs, payment anomalies, complaints, provider alerts, or traffic inconsistent with the declared use case can trigger renewed diligence.
- Refusal and suspension. Swifcom may refuse activation, restrict functions, require further evidence, or suspend or terminate service where identity, authority, intended use, or traffic cannot be satisfactorily verified.

4. Caller-ID authorization and anti-spoofing controls

- The platform restricts outbound caller-ID selection to numbers assigned or provisioned to the relevant account, or to external numbers whose possession or control has been verified and recorded.
- Account-level number assignments and caller-ID access determine which users and staff may present a number. A user cannot select an arbitrary caller ID merely by supplying a SIP header or application value.
- SIP and API traffic must authenticate using assigned credentials or an approved source-IP relationship. Application traffic must use an authenticated user or service context. Credentials can be revoked independently.
- Swifcom rejects, rewrites, or withholds outbound caller ID that is malformed, not authorized for the account, inconsistent with routing policy, or otherwise fails validation.
- When Swifcom cannot establish a customer's right to use a number, that number is not enabled as an outbound identity. Authorization can be withdrawn immediately if control changes or abuse is suspected.

5. Do-not-originate and number-validity controls

For calls within its control, Swifcom applies a reasonable do-not-originate policy consistent with 47 CFR 64.1200(o). It does not knowingly originate calls presenting invalid NANP numbers, unallocated numbers, numbers confirmed unused by the allocatee, or inbound-only numbers whose subscriber has requested that calls purporting to originate from the number be blocked. Number status and authorization are checked through Swifcom's provisioning records, customer verification records, carrier information, and notices received from numbering administrators, carriers, the FCC, law enforcement, or the Industry Traceback Group.

6. Traffic analytics and monitoring

Swifcom uses internal account, authentication, provisioning, routing, billing, and call-detail data to identify traffic that may be illegal or inconsistent with a customer's approved use. Swifcom does not currently rely on a separately contracted third-party robocall-analytics vendor. Contracted originating and terminating carriers may provide fraud, rejection, quality, reputation, or traceback signals; Swifcom treats those signals as inputs to, not substitutes for, its own mitigation program.

Indicators reviewed individually and in combination include:

- sudden or unexplained increases in call attempts, concurrency, or destination diversity;

- high-volume bursts, repetitive calling patterns, very short calls, low answer duration, or repeated dialing to sequential or concentrated number ranges;
- caller-ID changes, use of a number inconsistent with its assignment, failed authorization checks, malformed signaling, or attempts to bypass platform routing;
- traffic inconsistent with the customer's size, funded balance, history, declared use, geography, or expected operating hours;
- complaints, traceback requests, carrier warnings, elevated blocking or rejection responses, payment fraud indicators, or association with known illegal campaigns.

Monitoring is proportionate to risk and includes automated platform controls and human review. Swifcom may adjust indicators and thresholds as traffic, threats, provider feedback, and regulatory guidance evolve.

7. Investigation, mitigation, and escalation

When traffic is suspected of being illegal or abusive, Swifcom promptly correlates the affected calls with the responsible account, authenticated user or trunk, caller-ID authorization, payment record, routes, and upstream or downstream provider. Depending on urgency and evidence, Swifcom may:

- block the affected call, caller ID, destination, route, credential, trunk, user, or account;
- reduce channel capacity or rate limits, disable high-risk destinations, require manual approval, or place the account under enhanced monitoring;
- require the customer to explain the traffic and produce evidence of identity, number authorization, call purpose, and any legally required consent;
- suspend or terminate service where the customer does not respond promptly, the explanation is inadequate, or the traffic is illegal or presents an unacceptable risk;
- notify and coordinate with affected carriers, the FCC, law enforcement, or the Industry Traceback Group, and preserve relevant records.

A credible urgent notice involving ongoing illegal traffic is escalated immediately to the responsible officer. Swifcom will take effective mitigation within the period specified by the FCC or other competent authority and will not restore materially similar traffic until the risk is resolved.

8. Traceback response and cooperation commitment

Swift Mobile Solutions commits to respond fully and within 24 hours to every traceback request received from the FCC, law enforcement, or the industry traceback consortium, and to cooperate with those entities in investigating and stopping illegal robocallers that use its service to originate calls.

The RMD contact channel is monitored and escalated to personnel with access to account, call, routing, and provider records. A response will identify, to the extent available, the customer or account responsible for the call; the source user, application, API credential, IP-authenticated or registered SIP trunk; the presented caller ID and its authorization basis; timestamps and call identifiers; and the upstream or downstream carrier and route. If a complete answer cannot be assembled immediately, Swifcom will acknowledge and provide the available responsive information within 24 hours, continue the investigation without delay, and supplement the response promptly.

9. Records and evidence preservation

Swifcom maintains operational records sufficient to associate calls with accounts and routes, subject to applicable law and its retention policies. Relevant records include account and administrator identity, verified contact information, number provisioning and authorization, user and service credentials, IP or registration data where available, call-detail and billing data, routing and carrier data, complaints, alerts, investigation notes, mitigation actions, and traceback correspondence. When a complaint, alert, traceback, or investigation arises, relevant records are preserved from routine deletion for the duration reasonably necessary to respond and cooperate.

10. Upstream and interconnection-provider diligence

Swifcom knows the carriers and service providers from which it directly receives or to which it directly sends voice traffic. Before activating an interconnection or route, it records the provider's legal and operational identity, commercial contact, technical endpoints, service scope, and escalation path; confirms RMD status where the provider is required to file; and tests authentication and routing. Swifcom reviews provider notices, quality and fraud signals, traceback cooperation, and continued RMD status. It may restrict or cease a route or provider relationship where the provider presents an unacceptable illegal-traffic risk or fails to cooperate.

11. Governance and continuing review

- The responsible officer owns this program, the RMD contact, incident escalation, traceback performance, and coordination with technical and customer-service personnel.
- Personnel who activate accounts, numbers, credentials, trunks, or high-risk routes are instructed to apply the controls relevant to their role and escalate suspected abuse.
- The program is reviewed at least annually and after a material network, product, vendor, threat, enforcement, or regulatory change. The RMD filing is updated within 10 business days when required information changes and is recertified annually by March 1.
- When Swifcom obtains its own SPC token and certificate and implements STIR/SHAKEN, it will update this plan and its RMD implementation status within the required period.

12. Officer adoption

By filing this description with Swift Mobile Solutions' RMD certification, the signing officer confirms that the measures described above are in operation and that personnel responsible for the relevant systems and processes have been instructed to follow them. The filing officer must verify current configuration, vendor use, contact details, and operational practice before signing the RMD declaration under penalty of perjury.

Regulatory references

1. 47 CFR 64.6305(a), (d), (g), and (h), Robocall mitigation and certification.
2. 47 CFR 64.1200(n)(4) and (o), customer diligence and do-not-originate obligations.
3. FCC, DA 26-72, Wireline Competition Bureau Public Notice and Appendix A, released 22 January 2026: <https://docs.fcc.gov/public/attachments/DA-26-72A1.pdf>
4. FCC, DA 26-174, Enforcement Advisory 2026-02, released 20 February 2026: <https://docs.fcc.gov/public/attachments/DA-26-174A1.pdf>
5. FCC, FCC 24-135, Improving the Effectiveness of the Robocall Mitigation Database: <https://docs.fcc.gov/public/attachments/FCC-24-135A1.pdf>