Customer edition · Version 1.0 · 21 October 2026

Glacier Calling Privacy Security and Data Handling

Technical architecture and data lifecycle for calls routed through Glacier

---

Our purpose

Explain how Glacier Calling protects a call, what 3rd parties and carrier networks process, and how long operational records remain available.

Published by Glacier for customers, security teams, and privacy reviewers.

Executive summary

What Glacier Calling protects and where that protection ends

We use Twilio as the communications network and infrastructure provider for Glacier Calling. Our iOS and Android apps connect to Twilio's Voice infrastructure. Twilio then routes calls into or out of the public telephone network and the recipient's carrier, which may be AT&T, Verizon, T-Mobile, or another carrier. We do not operate the public switched telephone network.

We separate account identity from telecom routing. For calling identities covered by this paper, we generate a random UUID represented as hexadecimal text and use it as the Twilio client identity. We do not place the customer's name, email address, personal mobile number, address book, or hardware identifiers in that provider identity. Twilio still processes the Glacier number, the other party's telephone number, network addresses, an APNs VoIP push token, and call telemetry needed to place and support the call.

01

Transport encryption.

The app uses TLS for signaling and DTLS-SRTP for media to Twilio. Twilio terminates that encrypted transport, so a PSTN call is not end-to-end encrypted between both people.

02

Short diagnostics window.

We keep the Twilio Call Detail Record available for 48 hours so our support team can inspect call state, carrier and SIP errors, packet loss, jitter, latency, and related quality signals. We delete the Twilio Call resource when that window ends.

03

Seven-day synchronization window.

We mirror the app-facing call history and voicemail data in encrypted service storage for seven days. This gives a device time to download data after it has been offline or the app has not been opened.

04

User control.

A user can delete call history before the seven-day window ends. We delete the service copy, and our app clears its local encrypted records after the service confirms deletion.

How we anonymize account identifiers

Every telephone call creates routing and operational data. The network needs telephone numbers, timestamps, call direction, duration, network addresses, and service identifiers to connect and manage the call. Before we send a call into Twilio and the carrier networks, we replace the user's Glacier account identity with a randomly generated hexadecimal UUID. Twilio and downstream carriers receive the numbers and network data required to complete the call, but we do not send the user's Glacier name, email address, address book, or device hardware identifiers as part of that account identity.

What is a burner line and how should I use it

A burner line limits exposure of your primary phone number. For sensitive conversations with close, continuing contacts, use end-to-end encrypted voice calls.

A burner line is a separate phone number, often temporary, that lets people reach you without receiving your primary number. It can be useful even when you keep it for an extended period. Its main purpose is to control who has access to your everyday contact information.

Use

What it is used for.

Separating public-facing interactions from your personal life, managing temporary contacts, and reducing how widely your primary number circulates.

Use

What you should use it for.

Marketplace transactions, initial contact with unfamiliar people, service inquiries, event coordination, and other routine conversations where you need to be reachable without giving someone permanent access to your primary number.

Limit

What it does not provide.

A different number does not, by itself, make calls end-to-end encrypted or guarantee anonymity. Providers may retain activity records, including after a number is discarded.

Limit

What you should not use it for.

Do not rely on ordinary burner-line calls to protect confidential business discussions, sensitive personal matters, credentials, or private documents. Changing numbers does not address the confidentiality of the communication channel.

For continuing contacts

For family, close friends, colleagues, and other continuing contacts, establish an end-to-end encrypted platform as your normal channel for sensitive conversations. Use a service that protects voice calls by default, and place those calls inside the platform. End-to-end encryption is designed to keep conversation content audible only on the participants' devices.

FAQ

Glacier Calling frequently asked questions

What is Glacier Calling?

Glacier Calling lets you place and receive calls from the Glacier app using your Glacier number. We use Twilio as the communications network that connects our app to public telephone networks and carriers such as AT&T, Verizon, and T-Mobile.

How is a Glacier call routed?

Your device creates an authenticated, encrypted connection to the Twilio edge network. Twilio handles the signaling and media infrastructure, then routes the call through the public switched telephone network to the recipient's carrier.

For an incoming call, the process runs in reverse. The carrier delivers the call to Twilio, and Twilio sends it to the Glacier app.

Are Glacier calls encrypted?

Yes. The app uses TLS to protect call-control signaling and DTLS-SRTP to protect audio between your device and the Twilio edge network.

DTLS negotiates the cryptographic keys and connection parameters. SRTP encrypts and authenticates the audio packets while they travel between the Glacier app and Twilio.

Are calls end-to-end encrypted?

The connection between your device and the Twilio edge network is encrypted. Twilio terminates that encrypted connection so it can route the call to the public telephone network.

A standard call to a mobile or landline number is not end-to-end encrypted between both callers because the recipient's carrier does not use the same encryption keys established by the Glacier app.

Does every call create data?

Yes. Every telephone call creates routing and operational data. Telephone networks need information such as the calling and called numbers, timestamps, call direction, duration, network addresses, and service identifiers to connect and manage the call.

Glacier limits the account information attached to that data. We replace the user's Glacier account identity with a randomly generated hexadecimal UUID before connecting the call through Twilio.

How does Glacier anonymize my identity?

We generate a random hexadecimal UUID for each calling identity. We use that value as the Twilio client identity instead of the customer's name, email address, personal mobile number, advertising identifier, or device hardware identifier.

The UUID allows the calling system to deliver incoming calls and apply account-level controls without placing direct Glacier account information in the carrier route.

What information does Twilio process?

Twilio processes the information required to establish, route, operate, and troubleshoot a call. Depending on the call, this can include:

- The randomly generated Glacier UUID
- The assigned Glacier number
- The other party's telephone number
- Call SIDs and related service identifiers
- Call direction, status, timestamps, and duration
- Network addresses and Twilio edge information
- Packet loss, jitter, latency, codec, and other quality measurements
- An Apple Push Notification service token for incoming-call delivery

This information is used for calling operations. It is not used as a Glacier customer profile.

Does Twilio receive my name or email address?

We do not send your name or email address to Twilio as your calling identity. Twilio receives the randomly generated UUID used by the Voice SDK.

Does Twilio receive my personal mobile number?

We do not use your personal mobile number as your Twilio client identity.

A personal number can still become part of the telephone route if it participates in a call. For example, Twilio must process that number if you call your personal phone from Glacier or call your Glacier number from your personal phone.

Does Glacier upload my contacts to Twilio?

No. Contact matching happens on your device, but only if you give Glacier permission to access your contacts. The app compares calling numbers with your local contacts after it receives the call information.

Neither Twilio nor Glacier needs your complete address book to display a saved contact name in the app.

Does Twilio receive a device identifier?

Twilio does not receive hardware identifiers such as your device serial number, IMEI, IDFV, or advertising identifier from Glacier.

For incoming calls, Twilio processes an Apple Push Notification service token. Apple assigns this token to the Glacier app installation so an incoming-call notification can reach the correct device. It is not a hardware identifier, name, email address, or contact record.

Does Glacier have access to my carrier phone number, contacts, or voicemail?

No. Glacier does not have access to the phone number, contacts, or voicemail associated with your carrier account. Your carrier line and Glacier number operate separately.

What is a Call Detail Record?

A Call Detail Record is metadata about a call. It can include the calling and called numbers, status, direction, timestamps, duration, Call SID, routing information, failure codes, and quality measurements.

A Call Detail Record does not contain the audio from the conversation.

Why does Glacier keep Twilio call records for 48 hours?

The 48-hour window gives our support team enough time to investigate a newly reported calling problem.

During that period, we can use Twilio's APIs to review call status, SIP and carrier errors, packet loss, jitter, latency, connection failures, and other quality signals. These measurements help us determine why a call failed or had poor audio without listening to the conversation.

What happens after 48 hours?

We delete the completed Twilio Call resource through the Twilio REST API. Our retention worker confirms that Twilio completed the deletion and retries any record that is still finalizing or returns an error.

Once Twilio confirms the operation, the Call resource and its associated call events are no longer available through the Twilio API or Account Portal.

What calling data does Glacier store?

We keep an encrypted synchronization copy of the call history and voicemail data needed by the Glacier app for 7 days. This allows an authenticated device to download recent calls and voicemail after reconnecting to the service.

We protect this data with encryption in transit and encryption at rest.

Why does Glacier keep the synchronization copy for seven days?

A device may be powered off, disconnected, replaced, or unable to open the app immediately after a call. The seven-day window gives the device time to retrieve recent call history and voicemail.

If the device does not retrieve an item before the window expires, that item is deleted and cannot be recovered.

Can I delete my call history before seven days?

Yes. You can delete the call history for a Glacier number from the app at any time.

The app sends an authenticated deletion instruction to Glacier. We remove the server-side history, and the app removes the matching records from its local encrypted database after the service confirms the deletion.

What happens if a deletion fails?

The app reports the error and keeps the local record in place. It does not show a successful deletion while a server-side copy remains.

You can retry the deletion after the connection or service problem has been resolved.

How is call history protected on my iPhone?

The Glacier app stores downloaded call history in a SQLCipher-encrypted database. The database key is generated randomly and stored in the iOS Keychain rather than inside the database file.

Does Glacier record my calls?

No, we do not have any call recordings.

Voicemail is different. A voicemail is an intentional recording created when a caller leaves a message after an unanswered call. Voicemail is removed after 7 days, or immediately if the user chooses to delete it.

Can Glacier diagnose a call without hearing it?

Yes. We can investigate most calling problems using network and call-status data.

Packet loss, jitter, round-trip time, connection events, SIP responses, Twilio error codes, and audio-level measurements can identify many causes of failed calls, delayed audio, or one-way audio. These measurements do not contain the words spoken during the call.

Why does Glacier not support SMS text messaging?

A2P 10DLC (the carrier framework governing application-to-person texting) has effectively closed the door on anonymous or temporary SMS. Every registered messaging campaign now has to be tied to a verified legal entity (EIN/Tax ID) with a documented, traceable opt-in trail — which is the exact opposite of what a burner number is supposed to offer.

As of this year, carriers are outright blocking unregistered traffic at the network level, so texts sent through unregistered numbers get silently dropped before they reach anyone.

- **No path to registration:** the whole point of a burner number is anonymity, but 10DLC requires the opposite — real identity behind every campaign.
- **Number cycling is now penalized:** rotating through numbers to keep lines "fresh" (how most burner apps historically worked) is classified as "snowshoe messaging," and carriers can levy fines per violation.

Does Glacier Calling support emergency calls?

No. Glacier Calling is not an emergency calling service and should not replace the iPhone's native Phone app.

The Glacier iOS app blocks recognized emergency numbers from being converted into a Twilio calling request. Use the native Phone app to contact emergency services.

How we substantiate each technical statement

This paper expands the calling section of our iOS privacy and security whitepaper. It combines our iOS implementation reviewed on 21 October 2026, our current calling retention commitments, our public Privacy Policy, Twilio's product documentation, and the Internet standards that define DTLS-SRTP.

Evidence label	What it supports	What it does not prove
Glacier implementation	iOS SDK integration, authenticated API calls, local SQLCipher storage, local contact matching, and deletion behavior.	Live provider or production storage configuration beyond the reviewed client.
Glacier operating commitment	The 48-hour CDR deletion, seven-day encrypted sync mirror, and provider-facing UUID design described in this edition.	A Twilio default or an assurance that every provider derivative shares the same lifecycle.
Twilio documentation	Voice SDK connections, Access Tokens, push registration, Call resources, Voice Insights fields, and API deletion semantics.	Glacier-specific scheduling or Glacier service storage.
Internet standard	The role of DTLS in SRTP key establishment and SRTP's confidentiality, authentication, and replay protection.	End-to-end protection beyond the Twilio endpoint.
Documented boundary	A limit that follows from call routing, protocol termination, or separate data classes.	Independent penetration testing or certification.

Twilio is the network boundary between Glacier and the telephone system

A Glacier call is a direct encrypted socket from your device to the Twilio edge network. Our iOS app uses Twilio's Voice SDK to create an authenticated connection to a Twilio edge. Our services supply the token and call-control instructions. Twilio operates the signaling and media infrastructure and connects the call to the PSTN.

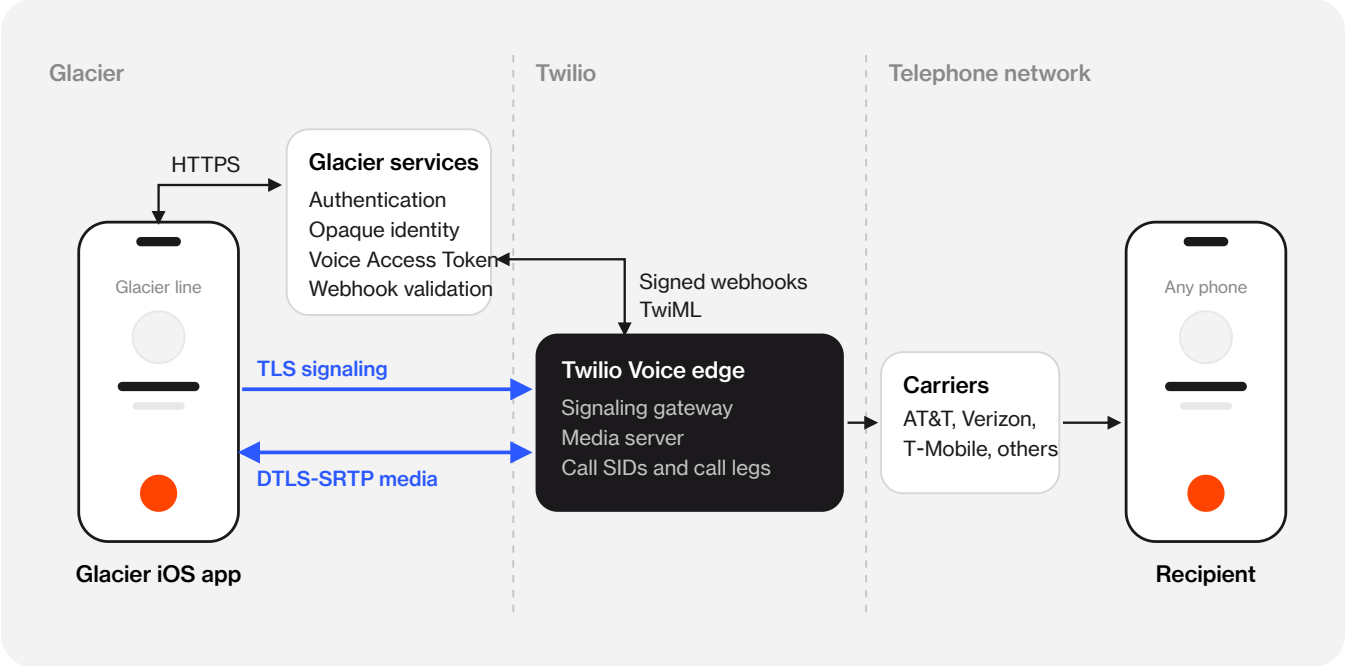


Figure 1. Glacier Calling crosses Glacier, Twilio, and telephone-network trust boundaries.

Operators in the path

- We authenticate the customer, map the account to an opaque calling identity, authorize the selected Glacier number, return a short-lived Voice Access Token, and handle signed Twilio callbacks.
- Twilio accepts the Voice SDK connection, terminates the app transport, creates call legs and Call SIDs, routes media and signaling, and interconnects with public telephone networks.
- The recipient's carrier completes the access-network leg. The exact carrier route can change and may include intermediary carriers.

Outgoing and incoming calls use different control paths

Outgoing call sequence

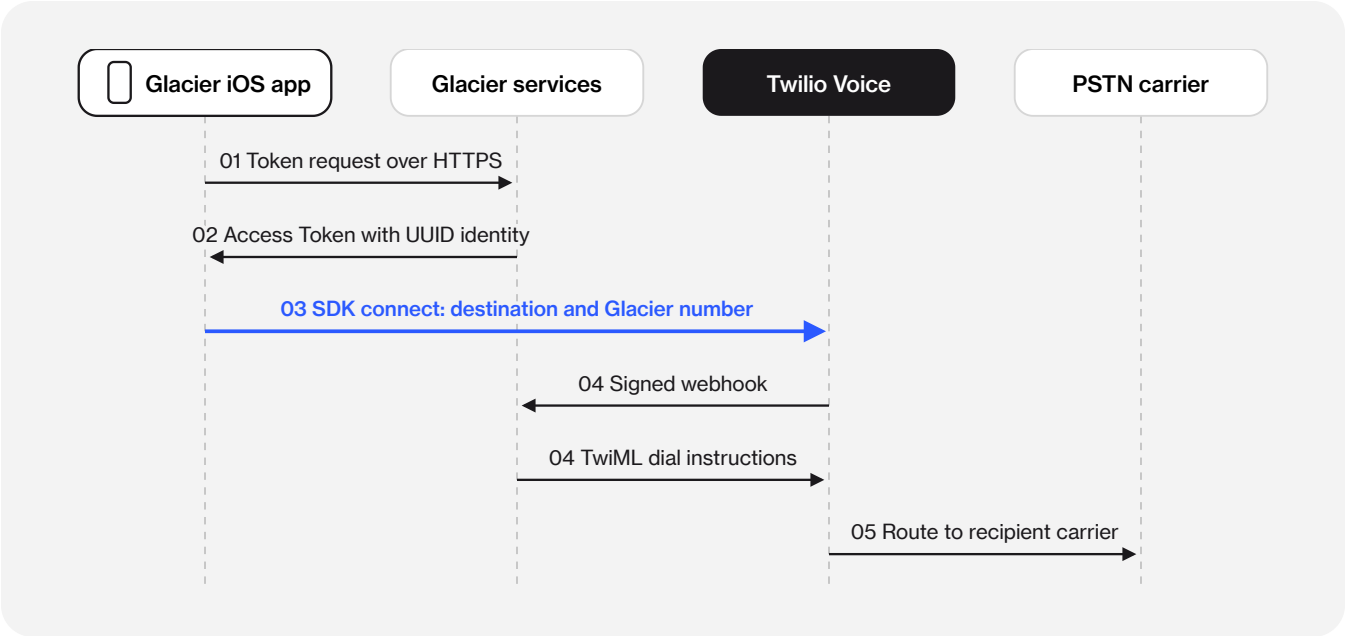


Figure 2. Outgoing call. Numbers match the steps below.

01 **Authenticate.** The signed-in app requests a Voice Access Token from Glacier through an authenticated HTTPS request.

02 **Issue an opaque identity.** We place the random hexadecimal UUID in the token's Voice identity grant, along with the TwiML application and permissions required for the session.

03 **Connect to Twilio.** The iOS app passes the destination number and the selected Glacier number to the Twilio Voice SDK. The SDK establishes signaling and media paths to Twilio.

04 **Authorize the route.** Twilio requests call-control instructions from our services. We validate the signed webhook, confirm the caller's number relationship, and return the TwiML needed to dial the destination.

05 **Reach the PSTN.** Twilio selects a route through its voice network and carrier interconnections. The recipient's provider completes the last network leg.

Incoming call sequence

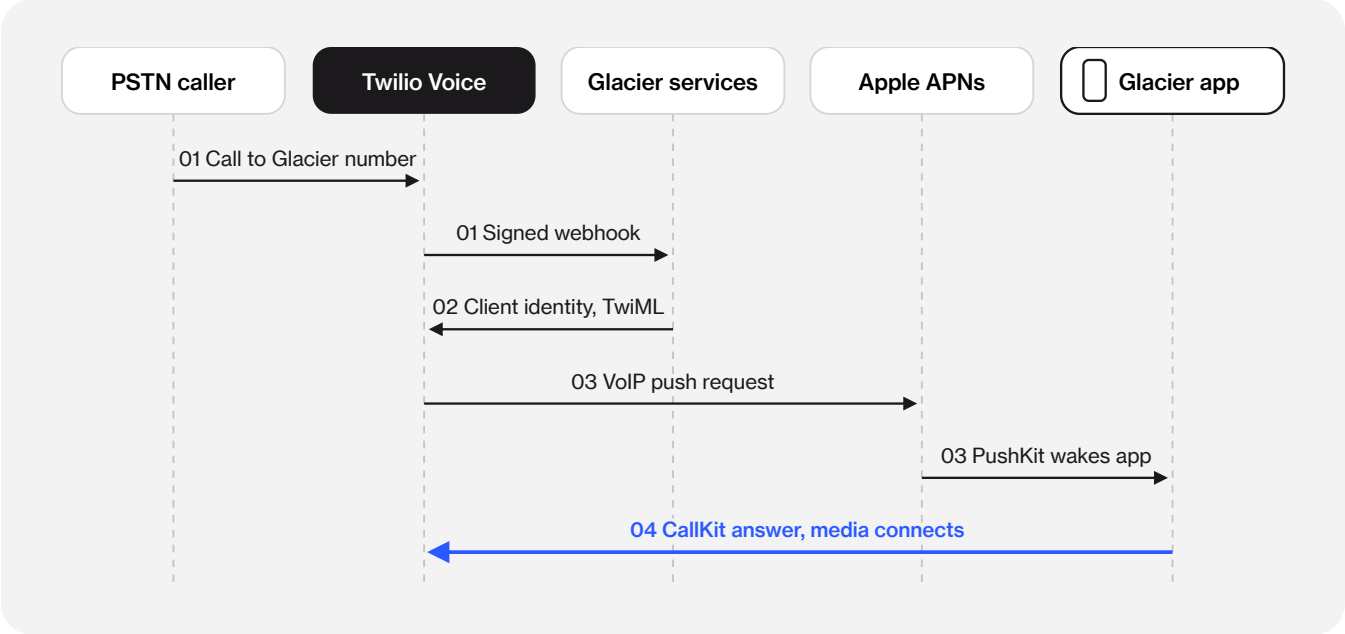


Figure 3. Incoming call. Numbers match the steps below.

01 **Receive the carrier call.** A caller reaches the provisioned Glacier number through the PSTN. Twilio receives the call and sends a signed webhook to Glacier.

02 **Resolve the account.** We map the provisioned number to the authorized opaque client identity and return the call-control response.

03 **Wake the app.** Twilio uses the registered APNs VoIP push token so Apple's PushKit service can wake the iOS app for the incoming call.

04 **Present and answer.** The Twilio SDK validates the invite path, our app reports the call through iOS CallKit, and the customer accepts or rejects the call.

Availability dependencies

Call setup requires Internet access, Glacier authentication and call-control services, Twilio Voice and push infrastructure, Apple Push Notification service for background incoming calls, and the downstream telephone network. A failure at any one of these points can prevent ringing or media even when the other systems are healthy.

The Twilio identity is an opaque random value

We create a per-account UUID and represent it as hexadecimal text for the Twilio client identity. The identifier is random. It is not an email hash, a phone-number hash, an advertising identifier, or a hardware identifier. We keep the internal mapping because our service must deliver incoming calls and apply account-scoped deletion.

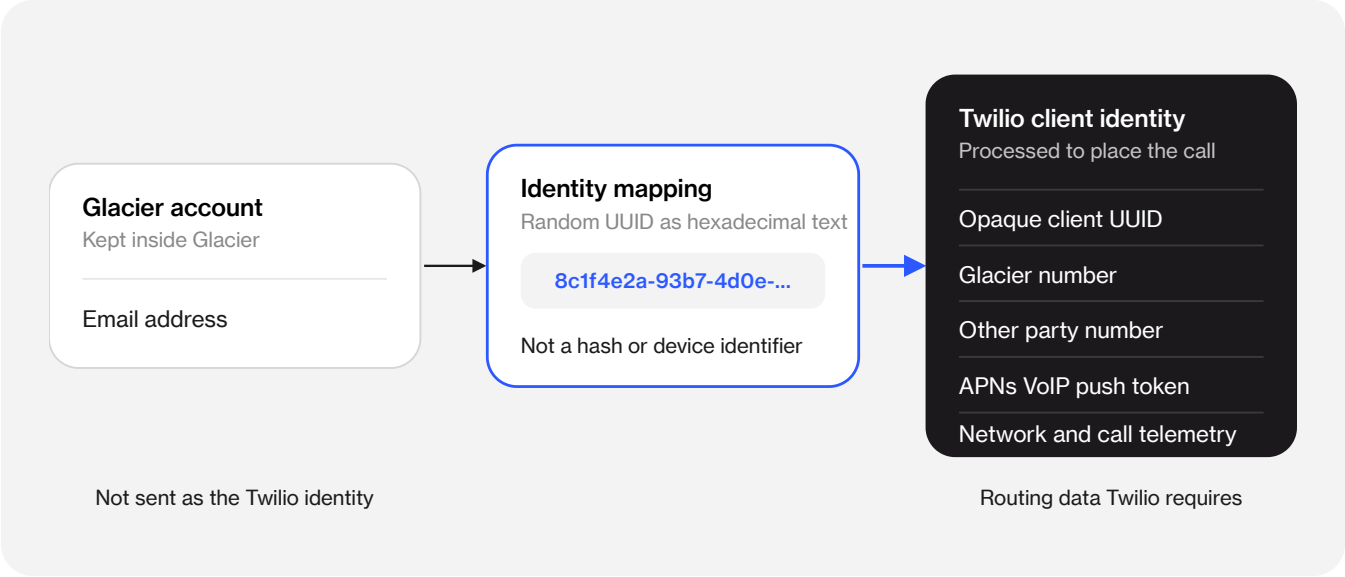


Figure 4. Glacier separates direct account identity from the Twilio client identity.

Routing data remains necessary even when profile data is removed

Data	Why Twilio receives it	Customer identity boundary
Opaque client UUID	Associates the Voice Access Token, registrations, and SDK call leg with the correct endpoint.	Random Glacier identifier, not the customer's name or email.
Glacier assigned number	Acts as the incoming number and supported caller ID for PSTN routing.	A service number provisioned for Glacier Calling.
Other party number	Routes an inbound or outbound PSTN call.	Required PSTN routing data, separate from the user's Glacier account identity.
Call SID and related SIDs	Identifies call legs and joins callbacks, status, history, and diagnostics.	Provider-generated service identifiers.
Timestamps, status, duration, direction	Operates the call, bills the service, displays history, and diagnoses failures.	Metadata that can reveal calling patterns.
Network addresses and edge data	Establishes signaling and media and measures connection quality.	Ordinary network metadata; not a Glacier hardware identifier.
APNs VoIP push token	Lets Twilio ask APNs to wake the iOS app for an incoming call.	A service token that identifies the app installation for push delivery.
SDK and quality telemetry	Measures codec, media path, packet loss, jitter, latency, audio levels, and call events.	Operational diagnostics, not call audio content.

Data not used as the Twilio profile identity

- Customer name and email address.
- The customer's personal mobile number, unless that number is itself dialed or presented by a PSTN participant in a particular call.
- Address-book contacts, local contact names, advertising identifiers, device serial number, IMEI, or IDFV.

Our app matches numbers to contact names on the device. Twilio and our call-history service receive telephone numbers needed for calling, but we do not upload the full address book for name matching.

TLS controls the call and DTLS-SRTP protects the audio transport

Signaling uses TLS to carry control information that registers the client, sets up the call, and reports state. Media uses SRTP. Twilio's network requirements identify the mobile media path as DTLS and SRTP over UDP, with TURN over TCP or TLS available when a restrictive network prevents a direct UDP path.

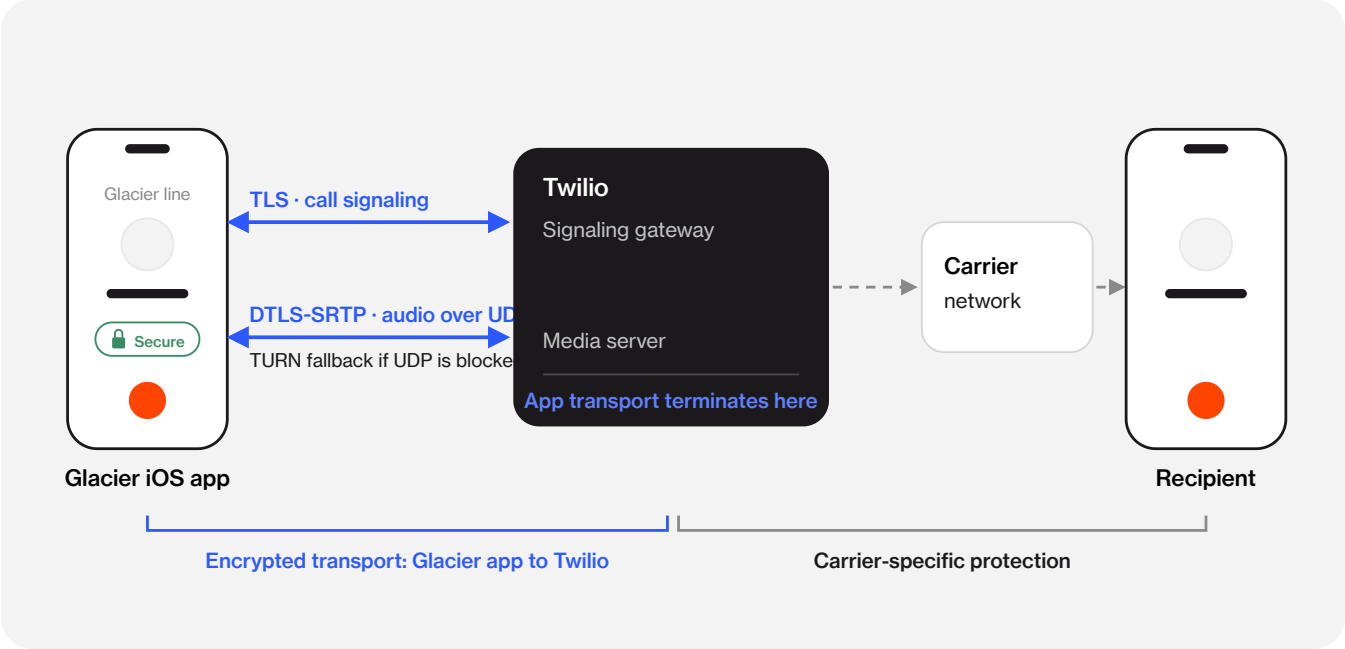


Figure 5. The encrypted app transport terminates at Twilio before the carrier leg.

What each protocol does

- **TLS** authenticates the Twilio signaling endpoint and protects call-control messages in transit between the SDK and Twilio.
- **DTLS** performs a handshake on the media path and establishes the keying material, algorithms, and parameters used by SRTP.
- **SRTP** protects RTP and RTCP traffic with confidentiality, message authentication, and replay protection, subject to the negotiated profile.

Transport encryption to Twilio is not caller-to-caller end-to-end encryption

Twilio must terminate the Voice SDK connection to route the call, connect multiple call legs, apply TwiML instructions, and interoperate with the PSTN. This makes Twilio part of the media trust boundary. The person on the other end does not hold the same SRTP keys negotiated by the Glacier app with Twilio.

Leg	Primary protection	Who terminates it	What remains outside
Glacier app signaling	TLS	Twilio signaling gateway	Twilio call control and downstream carrier signaling.
Glacier app audio	DTLS key establishment and SRTP media	Twilio media server	Twilio processing and every later call leg.
Twilio to carrier	Carrier-specific transport and interconnect controls	Twilio and downstream carrier	Recipient carrier and access network.
Carrier to recipient	Depends on carrier and endpoint technology	Recipient's carrier and device	No Glacier-controlled end-to-end key relationship.

Network traversal

ICE and STUN help the SDK find a working media path through NAT and firewalls. If direct UDP is blocked, TURN may relay traffic. A relay changes the packet route, not the Glacier identity model. SRTP still protects the media to the Twilio boundary.

Call audio and voicemail

A Call Detail Record is metadata, not an audio file. We do not use CDRs to store call content. Live media is relayed in real time and is not retained by us as a normal call recording. Voicemail is a separate, intentional recording created when a caller leaves a message after an unanswered call. It follows a separate content lifecycle.

Emergency calling

Glacier Calling is not an emergency calling service and should not replace the device's native cellular dialer. Our iOS client blocks recognized emergency numbers from being converted into a Twilio dial string. Customers should use the native Phone app for emergency services.

The record supports routing, history, billing, and problem diagnosis

Twilio creates a Call resource for each call leg. We use a subset of that record to display recent history and a separate diagnostic subset when a customer reports a problem. A Call SID is the primary correlation key.

Field group	Representative fields	Purpose
Correlation	Call SID, parent Call SID, account or subaccount SID	Join call legs, callbacks, diagnostics, and deletion requests.
Endpoints	To, From, formatted numbers, Twilio number SID	Route the call and display the correct Glacier line and other party.
State	Queued, ringing, in progress, completed, busy, failed, no answer, canceled	Explain what happened and drive the customer-facing history state.
Time	Created, updated, start, end, and duration	Order call history, calculate duration, and find the support window.
Direction	Inbound, outbound API, or outbound dial	Distinguish incoming and outgoing legs.
Failure	SIP response code, Twilio error code, disconnect reason	Separate authorization, destination, carrier, and network failures.
Route	Carrier edge, client edge, media region, signaling region	Identify where the call traversed Twilio infrastructure.
Quality	Packet loss, jitter, RTT, MOS, codec, audio levels, call tags	Diagnose degraded or one-way audio and failed media establishment.

Forty-eight hours preserves enough evidence to investigate a new call problem

Twilio can take up to 30 minutes to complete a Call Summary, while time-series metrics are typically available within about 90 seconds after a call. A 48-hour window gives the record time to finalize and gives a customer a practical period to report a failed or poor-quality call across time zones. It avoids turning call diagnostics into a long-term behavior archive.

Signal	What it can reveal	What it cannot prove alone
Packet loss	Missing media packets and the percentage lost on a measured edge.	Why packets were lost or exactly what the listener heard.
Jitter	Variation in packet arrival timing, including average and maximum values.	Whether the operating system, Wi-Fi, ISP, or carrier caused the variation.
RTT and latency	Round-trip or internal traversal delay on supported edges.	Full conversational delay across every carrier and endpoint.
MOS	A modeled voice-quality score derived from network conditions.	A person's subjective judgment of the call.
Audio input and output levels	Potential microphone, mute, speaker, or one-way-audio conditions.	The content of the conversation.
ICE and SDK events	Whether the client found a media path or failed during connection setup.	A carrier-side cause outside the SDK edge.
SIP and Twilio errors	Authorization, call-control, destination, and carrier failure classes.	A complete root cause without matching route and customer context.

Support access

Our support process starts with a narrow lookup using the approximate call time, Glacier number, direction, and Call SID when available. The purpose is to retrieve state and quality data for the reported call, not to browse a customer's calling patterns. We do not need call audio to diagnose packet loss, failure codes, or connection state.

Provider diagnostics and customer synchronization use different clocks

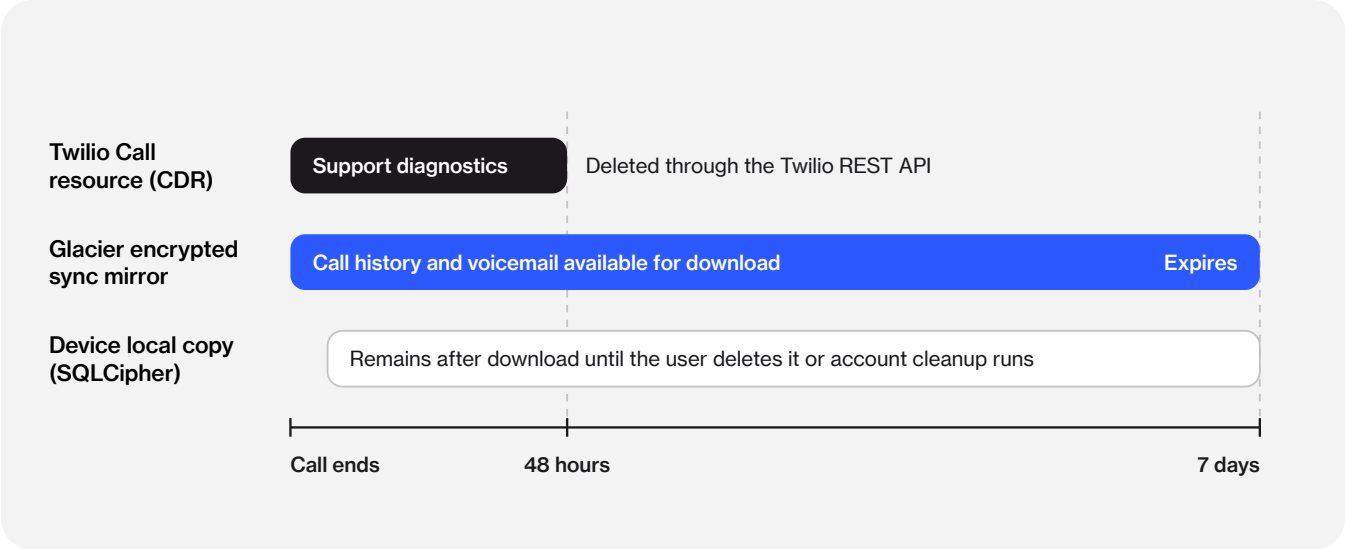


Figure 6. The 48-hour provider window and seven-day Glacier mirror serve different purposes.

At the 48-hour boundary

We delete each completed Twilio Call resource after 48 hours through the Twilio REST API. The deletion removes the call record from Twilio's API and Account Portal logs, together with the associated call events. Our retention worker confirms the deletion and retries any record that is still finalizing or returns an error. We do not mark the record deleted until Twilio confirms the operation.

Provider diagnostic boundary

The 48-hour deletion applies to the Twilio Call resources we use for Glacier call history and customer support. Voice Insights metrics are a separate Twilio diagnostic system with their own provider lifecycle. We use those metrics only to investigate call-quality and connection problems during the support window, and we do not mirror them into the customer's Glacier call history.

Seven days gives an offline device time to receive history and voicemail

We mirror the app-facing call-history and voicemail data required for synchronization in encrypted service storage for seven days. The mirror exists because a customer's device may be powered off, disconnected, replaced, or simply not open the app immediately after a call.

What the mirror is for

- Return incoming and outgoing history to the authenticated account.
- Provide voicemail metadata and authorized access to voicemail content.
- Allow the iOS app to download data into the device's encrypted local database.
- Preserve a short recovery window when an app launch or background refresh does not occur after the call.

What happens after seven days

The encrypted service mirror expires. If the app did not retrieve an item within the seven-day window, that item is deleted and cannot be recovered. A copy already synchronized to the device can remain locally until the user deletes it, the associated Glacier number is removed, account cleanup runs, or the application data is otherwise cleared.

Access control

The app uses an authenticated Glacier session to request history and voicemail for an account-owned Glacier number. The service derives or verifies ownership before returning records. A number supplied by the client is not treated as proof of authorization.

Encryption

We protect the mirror with encryption in transit and encryption at rest. The device stores downloaded call history in a SQLCipher database. Our app generates random database key material and keeps it in the iOS Keychain rather than inside the database file.

A manual delete shortens the Glacier lifecycle immediately

The user can delete call history for a selected Glacier number from the app. The app sends an authenticated deletion request to Glacier. Glacier verifies the number relationship and removes the server-side history even when the seven-day mirror has not expired.

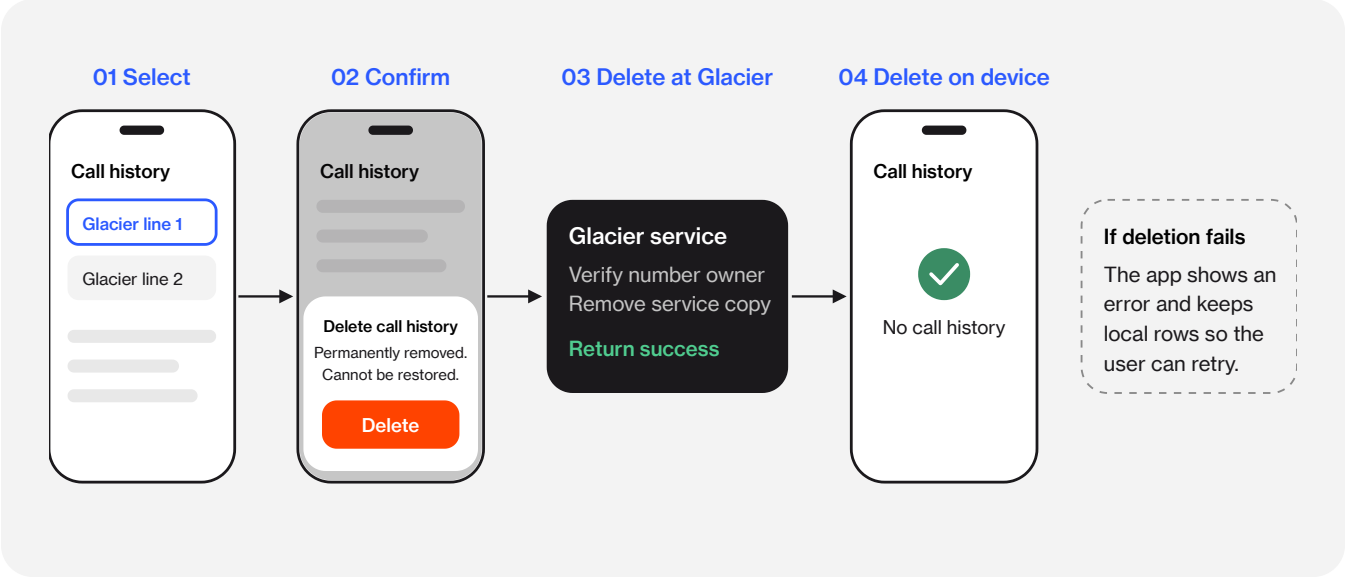


Figure 7. The device clears local rows only after Glacier confirms the service deletion.

01	**Select the number.** The user chooses the Glacier line whose history should be removed.
02	**Confirm the destructive action.** The app explains that the history will be permanently removed and cannot be restored through the Glacier service.
03	**Delete at Glacier.** The authenticated service request removes the number-scoped history from Glacier's service copy.
04	**Delete on the device.** Only after the service reports success does the app remove matching CallRecord rows from the local SQLCipher database.

Failure behavior

If the service deletion fails, the iOS app reports an error and does not pretend the operation succeeded by clearing only the visible local rows. This keeps the local state aligned with the server outcome and gives the user a chance to retry.

Voicemail audio and push tokens are separate data classes

Voicemail

Voicemail exists only when a caller leaves an audio message after an unanswered call. It includes audio content plus metadata such as the calling number, called number, Call SID, Recording SID, time, duration, and read or deleted state. A voicemail recording is not part of the Call Detail Record.

Incoming call push

To receive calls while the app is backgrounded or not running, iOS provides a PushKit device token. The Glacier app registers that token with Twilio together with the short-lived Voice Access Token. Twilio uses its configured APNs credential to ask Apple to deliver the incoming-call notification.

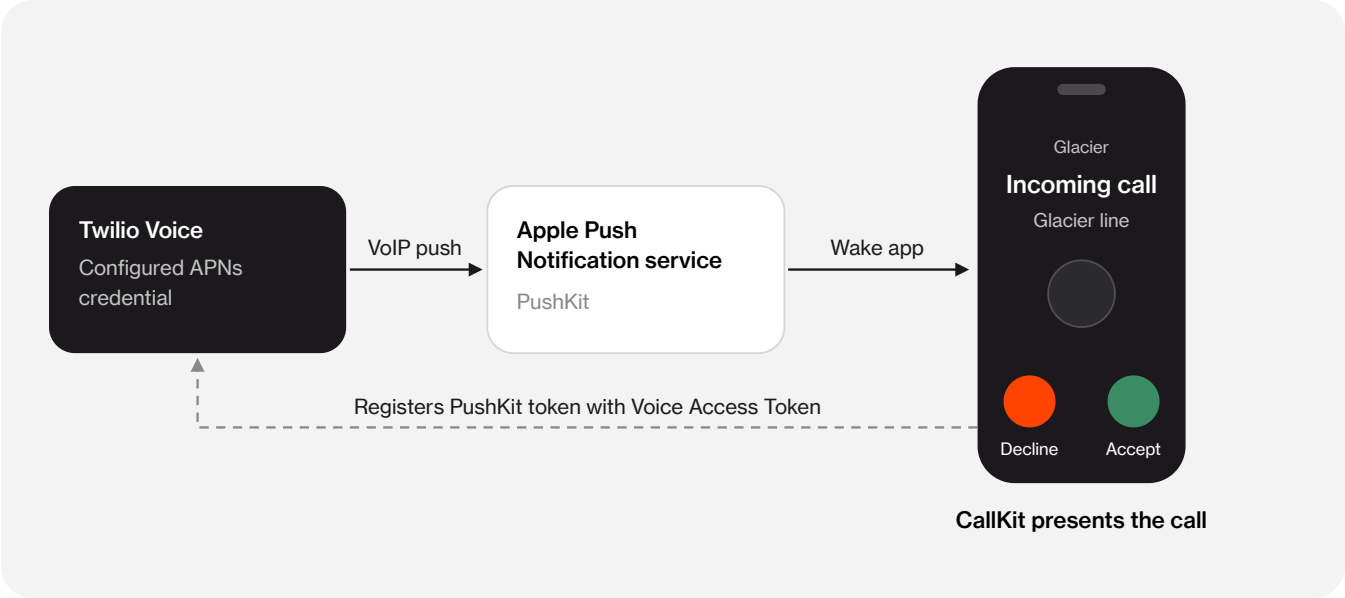


Figure 8. The registered push token lets Twilio wake the app through Apple for an incoming call.

The push token is a device or app-installation identifier for notification delivery. It is not the device's serial number, IMEI, IDFV, advertising identifier, contact list, name, or email address. It must still be treated as operationally sensitive and removed or refreshed when the app unregisters or the token changes.

Personal number boundary

We do not send the customer's personal mobile number to Twilio as the customer profile identity. The provisioned Glacier number is the supported caller ID. If a person chooses to call their Glacier number from a personal phone, or dials their personal phone as the destination, that number necessarily becomes PSTN routing data for that particular call.

Authentication, signatures, and least data limit the control plane

Short-lived access tokens

The iOS app receives a signed Twilio Voice Access Token from Glacier after authenticating to Glacier. The token contains the opaque identity, account and application identifiers, permissions, and expiration required by the SDK. It does not contain the customer's name or email as the Twilio identity.

Signed Twilio webhooks

Twilio signs HTTP requests with the X-Twilio-Signature header. We validate the signature against the exact public callback URL and the complete request parameters before trusting call-control or status data. HTTPS protects the webhook in transit; signature validation authenticates the sender and detects changed parameters.

Account-scoped retrieval

Call history and voicemail requests require a valid Glacier session. The service checks that the requested Glacier number belongs to the authenticated account before it returns or deletes records. Administrative access is separate and should be limited to support and security duties.

Local protection

The iOS client stores downloaded call history in the same SQLCipher-protected database used for local application records. Random key material resides in the iOS Keychain. Contact names are added locally after number matching, so the remote call record does not need the address-book label.

The design reduces identity exposure

Threat or concern	Control	Residual risk
Account identity exposed as SDK identity	Random hexadecimal UUID replaces direct name and email fields.	Glacier can resolve the UUID and metadata can still correlate activity.
Local network observes call audio	DTLS-SRTP protects the media transport from the app to Twilio.	Traffic analysis and endpoint compromise remain possible.
Long-term provider CDR availability	Glacier deletes Call resources after 48 hours.	Voice Insights, carrier records, billing data, or legal holds may follow separate lifecycles.
Offline device misses history	Encrypted Glacier mirror remains available for seven days.	A device offline longer than seven days may miss unsynchronized items.
Unauthorized history access	Authenticated account session and number-ownership checks.	A compromised account or unlocked device remains a risk.
Forged provider callback	HTTPS and X-Twilio-Signature validation.	Secret compromise or application validation defects remain risks.
Call recipient learns caller identity	Glacier number can separate the personal mobile number from caller ID.	Recipient sees the Glacier number; carriers and lawful authorities process routing metadata.
Device theft	SQLCipher local database and Keychain-held key material.	An unlocked or deeply compromised device can expose displayed data.

Appendix A

Control and evidence matrix

Control	Evidence basis	Customer-relevant boundary
Opaque UUID identity	Glacier operating commitment and provider-identity design	Pseudonymous; Glacier retains the account mapping.
Short-lived Voice Access Token	Glacier iOS flow and Twilio Access Token documentation	Twilio still knows the opaque identity and account context.
TLS signaling	Twilio Voice SDK network documentation	Protects only the app-to-Twilio signaling leg.
DTLS-SRTP media	Twilio network documentation and RFC 5764	Protects media to Twilio; not caller-to-recipient E2EE.
SRTP packet protection	RFC 3711	Confidentiality, authentication, and replay protection depend on negotiated profile and endpoint security.
48-hour CDR deletion	Glacier operating commitment and Twilio Call DELETE API	Call resource only; other provider data classes can differ.
Seven-day encrypted mirror	Glacier operating commitment	Short sync window; already-downloaded device data can remain.
Manual history deletion	Glacier iOS implementation and authenticated service flow	Removes Glacier and device copies in scope.
SQLCipher local database	Glacier iOS implementation	Protects copied storage when key material is unavailable; not an unlocked-device guarantee.
Local contact matching	Glacier iOS implementation	Called and calling numbers still enter the service route.
Signed webhooks	Glacier backend design and Twilio webhook security documentation	Depends on exact URL and full parameter validation.
VoIP push registration	Glacier iOS implementation and Twilio iOS documentation	Twilio processes the APNs token required for delivery.

Appendix B

Glossary

Term	Definition
Access Token	A short-lived signed JWT that authorizes a Voice SDK identity and its incoming and outgoing call permissions.
APNs VoIP push token	An Apple-issued token used to deliver incoming VoIP call notifications to a specific app installation.
Call Detail Record	Call metadata such as endpoints, state, time, duration, direction, identifiers, and selected routing or diagnostic fields.
Call SID	A Twilio-generated identifier for one call resource or call leg.
DTLS	Datagram Transport Layer Security. In DTLS-SRTP, the handshake establishes keying material and parameters for SRTP.
ICE, STUN, TURN	Network traversal mechanisms used to discover or relay a viable media path through NAT and firewalls.
MOS	Mean Opinion Score. A modeled voice-quality score based on measured network conditions.
Pseudonymous identifier	An identifier without a direct name.
PSTN	The public switched telephone network and its interconnected carrier systems.
SIP	A signaling protocol used in voice call setup, routing, and termination.
SRTP	Secure Real-time Transport Protocol. It protects RTP and RTCP with confidentiality, message authentication, and replay protection.
TwiML	Twilio Markup Language. Instructions returned by an application to tell Twilio how to handle a call.
Voice Insights	Twilio's call-quality analytics system for summaries, metrics, events, tags, and diagnostics.

Appendix C

Source basis and references

S1 **Glacier Privacy Policy.** Published calling-data categories, push-token disclosure, processor list, and customer controls.

S2 **Twilio Voice SDK overview.** Voice SDK architecture, Access Tokens, identities, TwiML applications, and status callbacks.

S3 **Twilio Voice iOS SDK getting started.** iOS Access Tokens, PushKit device-token registration, incoming calls, and client-to-PSTN calling.

S4 **Twilio Voice SDK network requirements.** TLS signaling, SRTP media, UDP DTLS-SRTP, media edges, and TURN fallback.

S5 **Twilio Access Tokens.** Identity grants, Voice grants, permissions, application SID, and push credential SID.

S6 **Twilio Call resource.** Call fields, status values, Call SIDs, retrieval, and DELETE semantics.

S7 **Twilio Call Summary resource.** Call metadata and cumulative quality metrics.

S8 **Twilio Call Metric resource.** Time-series packet loss, jitter, RTT, MOS, codec, and audio-level metrics.

S9 **Twilio Call Tags.** Diagnostic tags such as high packet loss, high jitter, and ICE failure.

S10 **Twilio Voice Insights frequently asked questions.** Provider retention and diagnostic behavior.

S11 **Twilio secure webhooks.** HTTPS and X-Twilio-Signature request validation.

S12 **RFC 5764 DTLS-SRTP.** DTLS key establishment and SRTP negotiation on the media path.

S13 **RFC 3711 SRTP.** SRTP confidentiality, message authentication, and replay protection.

Glacier implementation areas

- TwilioBackendManager, CallManager, Voice Access Token retrieval, Voice SDK registration, outgoing ConnectOptions, call history, voicemail, CallKit, and PushKit paths.
- CallRecord storage, SQLCipher database coordination, Keychain-held database key material, contact matching, number release, and call-history deletion flows.
- Glacier service identity translation, number ownership checks, Twilio webhook validation, encrypted synchronization storage, and retention workers.

Document history

Version	Date	Scope
1.0	21 October 2026	Initial Glacier Calling customer edition covering Twilio routing, identity minimization, DTLS-SRTP transport, CDR diagnostics, retention, synchronization, voicemail, and deletion controls.

Publication practice

We will revise this paper when the Twilio integration, protocol boundary, provider identity model, retention schedule, voicemail lifecycle, or user deletion behavior changes materially. The current Privacy Policy and product controls govern the service in use.