VEXERA

PUBLIC RELEASE · INDEPENDENT VALIDATION

Glacier App

Independent Validation of Privacy and Security Controls

November 4, 2026

ANDROID & IOS | NIST & NICE ALIGNED | INDEPENDENT VALIDATION

PREPARED FOR

Security App LLC
Glacier App · iOS & Android client

PREPARED BY

David De Jesus
Vexera Consulting LLC
david@vexeraconsulting.com

Overview

Glacier App is Security App LLC's privacy and secure communications application for iOS and Android. Vexera evaluated the technical controls behind its protected DNS, secure calling, encrypted routing, local data protection, and short retention model. This report summarizes the Glacier App capabilities Vexera validated and the user benefits those controls deliver.

Prepared by	Vexera Consulting LLC
Client	Security App LLC
Product	Glacier App
Validation period	October to November 2026
Validation focus	Android and iOS clients, protected DNS, secure calling, network routing, local data protection, and retention controls
Document status	Final release

Executive Summary

Vexera validated the core controls behind Glacier App's privacy and secure calling story: encrypted mobile transport, protected DNS using DNS-over-TLS, secure routing behavior, pseudonymous provider identities, local device safeguards, and a short data-retention model for calling records.

Across iOS and Android, Glacier App demonstrated a layered approach to privacy. The mobile clients protected traffic in transit, kept DNS activity on encrypted paths, protected local records with platform-backed storage controls, and supported a calling architecture designed to reduce unnecessary identity exposure. The product's calling lifecycle also reflects a clear minimization principle through a 48-hour Twilio call record window and a seven-day encrypted synchronization window for app-facing call history and voicemail data.

Key Conclusions

- Glacier App's external calling path is protected with encrypted signaling and media transport to Twilio's voice infrastructure.
- Glacier App's DNS protections were visible in runtime testing and source review, including DNS-over-TLS activity on iOS and protected DoT transport on Android.
- Glacier App's retention model reduces persistence of calling data through a 48-hour Twilio call-record window and a seven-day encrypted synchronization window.
- The Android and iOS clients use strong local protections, including encrypted storage, platform key protection, file protection, and secure network routing behavior.

How Vexera Validated Glacier App

Vexera combined mobile application review, connected-device testing, runtime observation, transport validation, and source-assisted control review to evaluate the controls behind Glacier App's public privacy and security claims.

VALIDATION AREA	REPRESENTATIVE ACTIVITIES	VALIDATED OUTCOME
Android mobile client	APK review, manifest review, storage inspection, certificate pinning checks, Firestack and WireGuard analysis, protected-route testing, and DNS transport review.	Confirmed secure Android posture, encrypted local storage, protected API boundaries, and DoT transport bound to the intended secure path.
iOS mobile client	Connected-device testing, entitlement review, NetworkExtension observation, file-protection review, TLS inspection, snapshot review, and Everyday and Travel mode testing.	Confirmed encrypted app traffic, DNS-over-TLS activity, secure tunnel behavior, production signing posture, and privacy-preserving device behavior.
Calling and retention controls	Review of Twilio Voice integration, authenticated calling flows, pseudonymous identity handling, call-history and voicemail lifecycle controls, and deletion paths.	Confirmed encrypted transport to Twilio, reduced direct identity exposure, and a short 48-hour and seven-day retention model.

Glacier App Capabilities Vexera Validated

Glacier App's privacy model is built from several coordinated control layers. Vexera validated the technical controls that support the product's public positioning across secure calling, protected DNS, short retention, pseudonymous provider identity, and mobile data protection.

GLACIER APP CAPABILITY	WHAT VEXERA VALIDATED	SECURITY AND PRIVACY BENEFIT
Encrypted external calling	Encrypted app traffic, Twilio Voice integration paths, TLS handshakes, SRTP media protection, and authenticated calling workflows.	Protects call signaling and media as they move from the device to Twilio's voice infrastructure.
Protected DNS	DNS-over-TLS activity on iOS, Android DoT transport through the protected WireGuard path, and secure DNS profile handling.	Keeps resolver traffic off plaintext network paths and supports privacy-focused filtering and safer browsing.
Short retention lifecycle	48-hour Twilio call-record deletion controls, seven-day encrypted synchronization storage, authenticated deletion behavior, and local encrypted history storage.	Limits the time operational calling data remains available while preserving support and device synchronization needs.
Pseudonymous provider identity	UUID-based provider identities for calling and managed DNS resources, protected API routes, and account-ownership checks in the reviewed workflows.	Reduces routine exposure of direct account identifiers and keeps provider interactions scoped to the authenticated customer context.
Mobile data protection	Android release signing, non-debuggable posture, backup restrictions, SQLCipher-backed records, Keystore-backed key protection, iOS file protection, and privacy-screened snapshots.	Protects local app state, calling history, and user information on the device.

Privacy and Security Outcomes

Glacier App's privacy posture is visible across the call path, DNS path, device state, and data lifecycle. Vexera observed measurable benefits across each of those layers.

CONTROL LAYER	WHAT VEXERA OBSERVED	USER BENEFIT
Calling confidentiality	The tested mobile flows used encrypted transports, and the reviewed calling architecture used TLS signaling and SRTP media to Twilio.	Helps keep call setup and media protected while they traverse the app-to-provider path.
DNS privacy	iOS testing showed DNS-over-TLS activity, while Android review confirmed DoT transport configured through the protected WireGuard route.	Reduces exposure of DNS activity on local and access networks.
Data minimization	The calling lifecycle used a 48-hour Twilio call-record window and a seven-day encrypted sync window for history and voicemail data.	Keeps operational records available only for the short period needed for support and synchronization.
Device privacy	Android used encrypted local storage and Keystore-backed key protection, while iOS used complete file protection, Keychain-backed secrets, and privacy screens.	Protects local records and reduces exposure from device loss, backup, or casual inspection.
Account privacy	Protected routes enforced authentication, provider-facing resources used UUID-based identities, and account-scoped ownership checks protected customer calling workflows.	Reduces direct identity exposure and supports privacy-preserving account interactions.

NIST and NICE Alignment

The clearest public-facing framework alignment for Glacier App is the NIST Cybersecurity Framework paired with the NIST Privacy Framework. Those frameworks describe the security and privacy outcomes Vexera observed. The NICE Workforce Framework complements that view by describing the assessment disciplines Vexera applied.

OBSERVED GLACIER APP EVIDENCE	RELEVANT NIST REFERENCE	HOW THE CONTROL ALIGNS
TLS and SRTP call transport, DNS-over-TLS activity, encrypted app traffic, and WireGuard-based routing.	CSF PR.DS-02 and PR.IR-01; Privacy Framework Protect-P.	These controls support protected data in transit, resilient network use, and privacy-preserving connectivity.
SQLCipher-backed records, Keystore and Keychain protection, iOS file protection, backup restrictions, and privacy-screened snapshots.	CSF PR.DS-01 and PR.PS-01; Privacy Framework Protect-P.	These controls support protection of local data and disciplined platform configuration.
UUID-based provider identities, authenticated routes, account-ownership checks, and protected deletion flows.	CSF PR.AA-03 and PR.AA-05; Privacy Framework Control-P and Protect-P.	These controls support authenticated access, scoped authorization, and data minimization across provider-facing workflows.
48-hour Twilio call-record deletion and seven-day encrypted synchronization storage.	Privacy Framework Control-P and Protect-P; CSF PR.DS-01.	These controls support purposeful data handling, shorter retention, and protection of stored operational records.

VEXERA ASSESSMENT DISCIPLINE	RELEVANT NICE WORK ROLE	HOW IT APPLIED
Mobile application review	Software Security Assessment	Vexera analyzed mobile application security controls, local storage, transport protection, and authentication behavior.
Network and transport validation	Systems Security Analysis	Vexera evaluated how VPN, DNS, and calling controls operated across device, network, and provider boundaries.
Attack-surface testing and revalidation	Vulnerability Analysis	Vexera tested exposed routes, protected flows, and previously reviewed control paths to confirm security behavior.

Why Glacier App Stands Out

Glacier App stands out because its privacy controls work together as a coordinated architecture. Encrypted calling transport protects sensitive communication paths. DNS-over-TLS reduces routine resolver exposure. Short retention windows limit how long calling records remain available, while pseudonymous provider identities reduce direct account exposure across the services that support the app.

The Android work showed a strong secure-mobile baseline through release signing, non-debuggable posture, backup restrictions, SQLCipher-backed records, Keystore-backed key protection, certificate pinning, and protected Firestack routing. The iOS work showed complete file protection, privacy-screened snapshots, encrypted app traffic, DNS-over-TLS activity, and stable NetworkExtension behavior.

The result is a product whose privacy story is backed by measurable controls. Glacier App protects network traffic, limits data persistence, separates direct identity from provider-facing resources, and preserves strong device-level safeguards across both major mobile platforms.

Conclusion

Vexera's validation work supports a clear public statement: Security App LLC has invested in the technical controls that matter most for Glacier App's privacy and secure communications model, and those controls performed well under independent assessment.

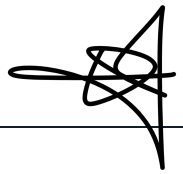
The strongest proof points were the encrypted app-to-Twilio calling path, DNS-over-TLS protections, short retention windows, pseudonymous provider identities, secure routing behavior, and the mobile data protections that help keep customer information protected on device.

Basis of Validation

This report is based on Vexera validation work performed during October and November 2026, including Android application review, iOS connected-device testing, VPN and DNS observation, transport validation, protected-route testing, and source-assisted review of calling, identity, and retention controls.

Validation Attestation

The validation summarized in this report was performed independently by Vexera Consulting LLC during October and November 2026. I attest that the results accurately reflect the controls observed during that assessment.



SIGNATURE

4 November 2026

DATE

David De Jesus

Penetration Tester / Red Team Operator · Vexera Consulting LLC