

Messaging App MVP

Comparable to: WhatsApp / Telegram

A lean mobile messaging app inspired by WhatsApp and Telegram. It provides private and group communication through text, media, and one-to-one voice calls.

Estimated MVP cost

\$25,150

Estimated effort

445 hours

To get your own customised cost for an app like this, visit www.chatstack.app and start a ChatStack interview describing how you want it customised.

Key Features

- Phone-number account creation with SMS verification.
- One-to-one text chat and group text chat.
- Media sharing and read receipts.
- One-to-one voice calls at launch.
- Push notifications and in-app account deletion.

Out of Scope for This MVP

- US-based hosting and privacy compliance.
- App Store and Google Play compliance.
- Free beta launch with no payment processing.
- Voice calling is limited to one-to-one calls for the MVP.
- No monetization is included during the beta.

Full Cost Breakdown

Item	Hours	Cost
The system shall allow a visitor to create an account using a phone number and shall use the phone number as the account identity.	5	\$280
The system shall send a one-time verification code by SMS and shall complete registration only when the code is valid and unexpired.	7	\$390
The system shall authenticate registered users by verified phone number and maintain an authenticated session for the mobile application.	7	\$390
The system shall allow authenticated users to send and receive one-to-one text messages associated with the conversation participants.	14	\$770
The system shall allow authenticated users to create user-defined group chats, manage membership, and send and receive group text messages.	20	\$1,100
The system shall allow users to attach and exchange supported photos and files within one-to-one and group conversations.	18	\$990
The system shall record and display read receipts for supported one-to-one and group messages.	10	\$550
The system shall allow authenticated users to initiate, receive, answer, decline, and end one-to-one voice calls.	25	\$1,380
The mobile application shall request microphone access only when a user initiates or answers a voice call and shall handle denied permission states.	5	\$280
The system shall send push notifications for new messages and incoming voice calls on supported iOS and Android devices.	16	\$880
The mobile application shall explain the purpose of notifications before requesting notification permission and shall handle denied permission states.	5	\$280
The system shall allow users to report users and objectionable text, media, and group content.	15	\$830
The system shall allow users to block and unblock other users and shall prevent blocked		

users from initiating or delivering prohibited interactions.

The system shall allow authenticated users to request account deletion within the application and shall provide a web-based deletion request process.	16	\$880
The system shall hard-delete associated account data after account deletion, except data subject to legally required retention.	19	\$1,050
Planning	48	\$2,640
Project Management	38	\$2,090
Testing	23	\$1,270
DevOps	19	\$1,050
Design & Frontend Build	58	\$3,190
AI Tokens	0	\$630
Security	23	\$1,270
Risk (10% Contingency)	42	\$2,310
Total	445	\$25,150

Estimate Assump tions

- Estimates cover application and backend de velopment across Flutter mobile and the specified web flow, excluding NFR overhead.
- Supabase, Twilio, OneSignal, FCM, managed storage, and a managed voice provider are available and used through standard SDKs or APIs.
- UI designs,

supported file types, size limits, retention rules, blocking policy, and deletion disclosures are provided during implementation.

-

Operational moderation staff and report-review procedures exist; the estimate covers the basic review queue rather than staffing.

- Voice calls use provider-managed signaling and media infrastructure; custom telecommunications infrastructure is excluded.

- Standard platform behavior is assumed for iOS and Android permissions, push delivery, and background execution.

- Hard deletion is implemented through application workflows and provider APIs; legal retention and backup purge policies are configuration dependencies.

Risks That Could Change This

- Voice-call behavior may expand if provider integration requires custom signaling, background-call handling, or platform-specific native work.
- Media scanning, large-file handling, and retention requirements may increase storage and processing implementation effort.
- Blocking rules for shared groups and existing conversations require product decisions before enforcement can be finalized.
- Account deletion may require additional compliance, audit, backup, or provider-specific deletion workflows.
- Push delivery and incoming-call reliability depend on Apple and Google platform restrictions and third-party service behavior.

User Stories

US-1 - Visitor

As a visitor, I want to create an account using my phone number so that I can use the messaging service.

US-2 - Visitor

As a visitor, I want to verify my phone number by SMS so that my account is protected from unauthorized registration.

US-3 - Logged In App User

As a logged-in app user, I want to send and receive one-to-one text messages so that I can communicate privately with another person.

US-4 - Logged In App User

As a logged-in app user, I want to participate in group text chats so that I can communicate with multiple people together.

US-5 - Logged In App User

As a logged-in app user, I want to share media in conversations so that I can exchange relevant photos and other supported files.

US-6 - Logged In App User

As a logged-in app user, I want to see read receipts for my messages so that I know whether recipients have viewed them.

US-7 - Logged In App User

As a logged-in app user, I want to make one-to-one voice calls so that I can speak privately with another person in real time.

US-8 - Logged In App User

As a logged-in app user, I want to receive notifications for new messages and incoming calls so that I can respond promptly.

US-9 - Logged In App User

As a logged-in app user, I want to report or block users and objectionable content so that I can control unwanted interactions and help maintain a safer community.

US-10 - Logged In App User

As a logged-in app user, I want to delete my account in the app and through a web request so that my account data is removed when I leave the service.

Requirements

FR-1 - Account Registration

The system shall allow a visitor to create an account using a phone number and shall use the phone number as the account identity.

FR-2 - Phone Verification

The system shall send a one-time verification code by SMS and shall complete registration only when the code

is valid and unexpired.

FR-3 - Authentication

The system shall authenticate registered users by verified phone number and maintain an authenticated session for the mobile application.

FR-4 - Direct Messaging

The system shall allow authenticated users to send and receive one-to-one text messages associated with the conversation participants.

FR-5 - Group Messaging

The system shall allow authenticated users to create user-defined group chats, manage membership, and send and receive group text messages.

FR-6 - Media Sharing

The system shall allow users to attach and exchange supported photos and files within one-to-one and group conversations.

FR-7 - Message Status

The system shall record and display read receipts for supported one-to-one and group messages.

FR-8 - Voice Calling

The system shall allow authenticated users to initiate, receive, answer, decline, and end one-to-one voice calls.

FR-9 - Device Permissions

The mobile application shall request microphone access only when a user initiates or answers a voice call and shall handle denied permission states.

FR-10 - Notifications

The system shall send push notifications for new messages and incoming voice calls on supported iOS and Android devices.

FR-11 - Notification Permissions

The mobile application shall explain the purpose of notifications before requesting notification permission and shall handle denied permission states.

FR-12 - Safety and Moderation

The system shall allow users to report users and objectionable text, media, and group content.

FR-13 - User Blocking

The system shall allow users to block and unblock other users and shall prevent blocked users from initiating or delivering prohibited interactions.

FR-14 - Account Deletion

The system shall allow authenticated users to request account deletion within the application and shall provide a web-based deletion request process.

FR-15 - Data Deletion

The system shall hard-delete associated account data after account deletion, except data subject to legally required retention.

NFR-1 - Performance

The system shall target API response times below 200 milliseconds for standard synchronous requests under expected beta load.

NFR-2 - Scalability

The backend shall use a managed database platform capable of scaling with beta users, conversations, messages, and media metadata.

NFR-3 - Observability

The mobile application and backend shall provide performance monitoring, error tracking, and operational logs sufficient to diagnose core user journeys.

NFR-4 - Security and Privacy

The system shall protect account, message, media, call, and report data through authenticated access control, encryption in transit, and least-privilege authorization.

NFR-5 - Availability and Reliability

The system shall provide reliable message, notification, media, and call services with retry or recovery handling for transient failures.

NFR-6 - Platform Compatibility

The mobile application shall support current target versions of iOS and Android and shall comply with applicable platform permission and store policies.

Requirements Assumptions

- The MVP consists of iOS and Android mobile applications plus a web account-deletion request flow.
- No third-party integrations are included except SMS delivery, push notifications, voice calling infrastructure, media storage, and monitoring services.
- Phone numbers are unique account identifiers and SMS verification is available in the launch markets.
- Messages and shared media are accessible only to intended conversation participants, subject to moderation and legally required access.
- The beta supports text messages, photos, and a defined subset of file types with configurable size limits.
- Voice calling is one-to-one only at launch; video calling, conferencing, and call recording are excluded.
- User-created groups support multiple members, with membership and administrative rules defined during detailed design.
- Basic reporting and blocking are in scope; staffing and procedures for operational report review are project dependencies.
- Account deletion is immediate hard deletion by default, subject to legal retention, backups, fraud prevention, and audit requirements.
- The service is free at launch and has no payments, subscriptions, advertising, or in-app purchases in the current scope.
- Supabase-managed database infrastructure and Firebase Performance Monitoring are the baseline technology assumptions.
- Specific capacity, availability targets, retention periods, supported regions, and minimum device versions will be finalized during estimation and architecture.

Technical Specification

TS-1 - Mobile Application

Build iOS and Android applications with Flutter and Dart, using Riverpod for state management and Material Design 3 for the UI system.

TS-2 - Authentication

Use Supabase Auth with JWT-based sessions and Twilio SMS verification for phone-number registration and authentication.

TS-3 - Authorization and Access Control

Implement server-enforced authorization for conversations, groups, media, calls, reports, blocking, and account deletion using authenticated user identity and least-privilege rules.

TS-4 - Backend and API

Provide a REST API over HTTPS using Supabase-managed backend capabilities, PostgreSQL, and optional edge functions for asynchronous or privileged operations.

TS-5 - Data Storage and Media

Use Supabase-managed PostgreSQL for accounts, conversations, messages, groups, receipts, calls, reports, and deletion state; use managed object storage for media files and metadata.

TS-6 - Real-Time Communication

Implement near-real-time message and presence updates through backend-supported realtime mechanisms and integrate a managed one-to-one voice-calling provider.

TS-7 - Notifications

Use OneSignal and Firebase Cloud Messaging for push notifications on iOS and Android, with deep links to messages and incoming calls.

TS-8 - Web and Admin UI

Build a Next.js, React, and TypeScript web application using shadcn/ui and Tailwind CSS for account-deletion requests and administrative report review.

TS-9 - Hosting and Environments

Host web and admin applications on Vercel and use Supabase-managed infrastructure for database and backend services; maintain development, staging, and production environments.

TS-10 - CI/CD and Testing

Use GitHub Actions for backend and web pipelines and CodeMagic for mobile build and store-release workflows, with unit, integration, and end-to-end testing.

TS-11 - Security and Privacy

Protect data with TLS 1.2+, encrypted managed storage, JWT authentication, least-privilege authorization, secure secrets management, and privacy-aware deletion controls.

TS-12 - Observability and Operations

Provide centralized application logs, error tracking, performance monitoring, audit events, service health checks, and alerting for core user journeys and integrations.

TS-13 - Moderation and Account Lifecycle

Implement report submission, blocking, operational review queues, account-deletion requests, hard-deletion processing, and legally required retention exceptions.

Technical Assumptions

- The MVP includes Flutter iOS and Android applications plus a Next.js web flow for account-deletion requests and administration.
- Supabase Auth, PostgreSQL, storage, and optional edge functions are the baseline backend technologies.
- Twilio is used for SMS verification; OneSignal and Firebase Cloud Messaging are used for push notifications.
- Vercel hosts web and admin applications; GitHub Actions and CodeMagic provide CI/CD automation.
- Development, staging, and production environments are provisioned separately with isolated credentials and data.
- Phone numbers are unique account identifiers and SMS delivery is available in the launch markets.
- Voice calling is provided by a managed third-party service and supports one-to-one calls only at launch.
- Media storage, supported file types, size limits, retention, and scanning rules are configurable beta policies.
- Admin roles are limited to authorized operational staff and all privileged actions are auditable.
- Account deletion is immediate hard deletion by default, subject to legal retention, backups, fraud prevention, and audit requirements.
- Data residency, supported regions, minimum mobile OS versions, capacity targets, and uptime objectives are finalized during architecture and estimation.
- The service has no payments, subscriptions, advertising, or in-app purchases in the current scope.

To get your own customised cost for an app like this, visit <https://www.chatstack.app> and start a ChatStack interview.

This is a starting estimate for a custom-built MVP, designed and built from scratch. You own all the code and IP with no platform lock-in. WhatsApp / Telegram are trademarks of their respective owners; ChatStack / App Developer Studio is not affiliated with, endorsed by, or sponsored by WhatsApp / Telegram. © 2026 ChatStack. Created with ChatStack (www.chatstack.app)