

Privacy Policy

Effective Date: 05/03/26

App Name: ServiceLine

Company Name: StringinLLC

Contact Email: contact@servicelinellc.com

StringinLLC (“ServiceLine,” “we,” “us,” or “our”) respects your privacy. This Privacy Policy explains how we collect, use, store, share, and protect information when you use our website, mobile application, platform, services, and related features collectively referred to as the “Service.”

By using the Service, you agree to the collection, use, and sharing of information described in this Privacy Policy.

This Privacy Policy applies to customers, stringers, waitlist users, website visitors, and other users of the Service.

1. Information We Collect

We may collect the following categories of information depending on how you use the Service.

Account and Personal Identifier Information

When you create an account, join our waitlist, use the Service, or interact with us, we may collect personal identifiers such as:

- Name
- Firebase Auth display name
- Email address
- Phone number
- Username
- Password or authentication credentials
- Profile information
- Profile photo
- Firebase user ID, also known as a UID
- User type, such as customer, stringer, player, or other role
- Other information you choose to provide

We may use your Firebase UID as the document ID or account identifier for customer or stringer records in our database.

Authentication Information

We may use Firebase Authentication to help create, manage, and secure user accounts. Depending on how you sign up or log in, Firebase Authentication may process information such as your name, email address, phone number, authentication credentials, phone verification information, and Firebase UID.

If phone number verification is used, we may use phone one-time password authentication, also known as phone OTP.

Location Information

Because our Service connects users based on nearby availability, we may collect location information, depending on your device settings, app permissions, and how you use the Service.

For customers, we may collect information such as:

- Zip code
- Approximate location
- Location information used to match customers with nearby stringers

For stringers, we may collect information such as:

- Service area
- Latitude and longitude
- Service radius
- GeoFire or similar geolocation data stored in Firestore

We may use location information to:

- Show nearby stringers or customers
- Help users coordinate services
- Improve matching and app functionality
- Help prevent fraud or misuse
- Improve safety and reliability
- Display relevant availability or service areas

You can control location permissions through your device settings. However, some features of the Service may not work properly without location access.

Payment and Financial Information

We use Stripe to process payments, payouts, identity verification, fraud prevention, and related financial services.

For customers, Stripe may collect and process payment-related information such as:

- Card number
- Expiration date
- CVV
- Billing address
- Payment method information
- Stripe Customer ID
- Transaction information
- Fraud prevention and risk signals

For stringers receiving payouts through Stripe Connect Express, Stripe may collect and process additional information such as:

- Full legal name
- Date of birth
- Social Security number, including the last four digits or full number when required
- Home address
- Bank account and routing number
- Stripe Connect account ID
- Tax information
- Identity verification information

If Stripe Identity is used during stringer onboarding, Stripe may collect information such as:

- Government-issued identification, such as a driver's license or passport;
- Selfie or biometric verification information;
- Identity verification results;
- Other information required for verification, fraud prevention, legal compliance, and payout eligibility.

We do not store full card numbers, CVV codes, complete bank account numbers, or full identity verification documents on our own servers. This information is generally collected and processed by Stripe. However, we may transmit certain information to Stripe or receive limited payment-related identifiers from Stripe, such as Stripe Customer IDs, Connect account IDs, Payment Intent IDs, transfer IDs, payout status, fee information, or transaction status.

Transaction, Order, and Service Information

We may collect information related to services requested, purchased, or provided through the Service, including:

- Racket stringing requests
- Racquet count
- String brand
- String type
- Tension preferences

- Main and cross tension
- Turnaround type
- Service details
- Drop-off information
- Pickup information
- Order timeline
- Drop-off timestamps
- Pickup timestamps
- Completion timestamps
- Order status
- Order history
- Pricing
- Platform fees
- Fee breakdowns
- Refunds
- Transaction history
- Payment Intent IDs
- Transfer IDs
- Dispute or support information
- Customer and stringer communications related to the order

Reviews, Ratings, and User Content

If you leave a review, rating, comment, profile description, image, message, or other content in the Service, we may collect, store, process, and display that content as part of the Service.

This may include:

- Review rating
- Review text
- Profile photo
- Profile description
- Uploaded images
- Messages
- Other user-generated content

Reviews, ratings, and some profile information may be visible to other users.

Communications and Messaging

If you contact us for support, send us feedback, communicate with other users, or use messaging features in the Service, we may collect the content of those communications and related information.

This may include:

- In-app messages between customers and stringers
- Firestore messages
- Support requests
- Feedback
- Message timestamps
- Message sender and recipient information
- Push notification tokens, including Firebase Cloud Messaging tokens stored per user

Device, Technical, Analytics, and Diagnostic Information

We may automatically collect certain technical, usage, analytics, and diagnostic information when you access or use the Service, including:

- IP address
- Device type
- Device model
- Browser type
- Operating system
- OS version
- App version
- Log data
- Screen views
- Pages or features used
- Date and time of activity
- Crash reports
- Stack traces
- Custom crash or diagnostic keys
- Referral information
- App performance data
- General usage analytics
- Device identifiers
- Firebase app instance ID
- Push notification tokens
- Security-related logs

We may use Firebase Crashlytics to collect crash logs, device model, OS version, app version, stack traces, custom keys, and related diagnostic information.

We may use Firebase Analytics, including Google Analytics for Firebase, to collect app analytics information such as app instance ID, screen views, product interactions, custom events, and user properties.

Examples of analytics events we may collect include:

- Sign-up events

- Login events
- Begin checkout events
- Order submitted events
- Review submitted events
- Message sent events
- User type, such as customer or stringer

Apple Search Ads and Apple Services Information

If you install or interact with our app through Apple services, we may receive information from Apple or Apple-related tools, such as:

- Apple Search Ads attribution token
- Install-source attribution information
- App Store Connect analytics
- Apple Push Notification Service information needed to deliver notifications
- Other information provided by Apple in accordance with Apple's terms and privacy practices

We may use Apple Search Ads attribution information to understand whether an app install came from Apple Search Ads and to measure marketing performance.

Website and Hosting Information

If you visit our website, we or our hosting providers may collect website-related information such as:

- IP address
- Request logs
- Browser type
- Device information
- Pages visited
- Date and time of request
- Referring pages
- Other technical information

We use Vercel for website hosting. Vercel may receive IP addresses, request logs, and related technical information when users visit our website.

Waitlist and Marketing Information

If you join our waitlist, sign up for updates, or interact with marketing communications, we may collect information such as:

- Email address

- Name, if provided
- Role, such as player, customer, or stringer
- Marketing preferences
- HubSpot contact properties, if HubSpot is connected or used
- Communication history
- Waitlist signup information

We may currently store waitlist information in Firestore and may later sync or store waitlist and marketing information in HubSpot.

2. How We Use Your Information

We may use your information to:

- Provide, operate, maintain, and improve the Service
- Create, authenticate, and manage user accounts
- Connect customers with stringers
- Display nearby stringers or relevant service areas
- Process bookings, orders, service requests, and order updates
- Process payments, payouts, refunds, fees, and disputes
- Verify identity or eligibility where needed
- Support Stripe Connect onboarding and Stripe Identity verification
- Enable location-based matching
- Display reviews, ratings, profiles, and user-generated content
- Store and manage text, images, messages, profile content, reviews, and other user-generated content
- Enable in-app messaging between customers and stringers
- Send push notifications, booking updates, reminders, service messages, security notices, and support communications
- Send marketing or promotional messages where permitted by law
- Manage waitlists and marketing contacts
- Analyze app usage, product interactions, performance, and user engagement
- Measure install attribution and marketing effectiveness
- Improve app performance, design, reliability, and user experience
- Diagnose bugs, crashes, technical errors, and performance issues
- Maintain app security, enforce security rules, and help prevent unauthorized access
- Detect, prevent, and investigate fraud, abuse, theft, misuse, security issues, or illegal activity
- Enforce our Terms of Service and other policies
- Resolve disputes between users
- Provide customer support
- Comply with legal, tax, accounting, regulatory, and law enforcement obligations
- Protect the rights, property, safety, and security of ServiceLine, users, service providers, and others

3. How We Share Information

We may share information in the following situations.

With Other Users

To make the Service work, we may share certain information between customers and stringers, such as:

- Name
- Username
- Profile photo
- Profile information
- User type
- Approximate or relevant location information
- Stringer service area
- Service request details
- Order details
- Drop-off, pickup, or coordination details
- Ratings and reviews
- Messages or communications
- Order status and timeline information

For example, a customer may need to see information about a nearby stringer, and a stringer may need to see information about a customer's service request in order to complete the order.

With Google Firebase

We use Google Firebase for app infrastructure and functionality, including Firebase Authentication, Firestore, Firebase Storage, Firebase Cloud Messaging, Firebase Crashlytics, Firebase Analytics, Remote Config, Cloud Run, security rules, and related services.

Firebase may process personal information, account information, device information, analytics data, diagnostic data, user-generated content, messages, images, notification tokens, location-related data, security logs, and other information necessary to provide these services to us.

We use Firebase to:

- Authenticate users
- Store user records
- Store text, images, messages, reviews, and profile content
- Store waitlist information
- Send and manage push notifications
- Analyze app activity and product interactions

- Monitor crashes and app performance
- Enforce security rules and access controls
- Support backend functions and app infrastructure
- Improve reliability, security, and user experience

Google may process information in accordance with its own privacy practices, legal terms, and data processing terms.

Google Firebase Privacy and Security information is available here:

<https://firebase.google.com/support/privacy>

Google Privacy Policy is available here: <https://policies.google.com/privacy>

With Stripe

We use Stripe for payment processing, Stripe Connect, payouts, fraud prevention, disputes, tax-related reporting, and identity verification.

We may share payment, transaction, customer, stringer, order, fee, refund, payout, dispute, and identity-related information with Stripe so Stripe can provide these services.

Stripe may also collect information directly from users when they enter payment information, complete checkout, onboard for payouts, verify identity, or provide tax or banking information.

Stripe's Privacy Policy is available here: <https://stripe.com/privacy>

Stripe's Privacy Center is available here: <https://stripe.com/legal/privacy-center>

With Apple

We may share or receive information through Apple services when you use the app on Apple devices or interact with Apple-related services.

This may include information related to:

- Apple Search Ads attribution
- App Store Connect analytics
- Apple Push Notification Service
- App installation and app performance information
- Other Apple platform services used to operate or distribute the app

Apple may process information according to its own privacy practices and legal terms.

Apple Privacy Policy is available here: <https://www.apple.com/legal/privacy/>

Apple App Privacy Details information is available here:
<https://developer.apple.com/app-store/app-privacy-details/>

With HubSpot

We may use HubSpot for waitlist management, marketing communications, customer relationship management, contact organization, and related marketing or support purposes.

If HubSpot is connected or used, we may share or store information such as:

- Name
- Email address
- Role, such as player, customer, or stringer
- Waitlist information
- Marketing preferences
- Contact properties
- Communication history

HubSpot may process information according to its own privacy practices and legal terms.

HubSpot Privacy Policy is available here: <https://legal.hubspot.com/privacy-policy>

With Vercel

We use Vercel for website hosting and related website infrastructure.

When you visit our website, Vercel may receive technical information such as:

- IP address
- Request logs
- Browser information
- Device information
- Pages visited
- Date and time of request
- Other information necessary to provide hosting, security, performance, and website infrastructure services

Vercel may process information according to its own privacy practices and legal terms.

Vercel Privacy Policy is available here: <https://vercel.com/legal/privacy-policy>

With Other Service Providers

We may share information with vendors and service providers who help us operate, secure, improve, and provide the Service, such as:

- Hosting providers
- Cloud storage providers
- Analytics providers
- Customer support tools
- Email providers
- Messaging providers
- Push notification providers
- Security providers
- Fraud prevention providers
- Payment processors
- App performance and crash reporting tools
- Marketing tools
- Development and infrastructure providers

These providers are allowed to use information only as necessary to provide services to us, unless otherwise permitted by law.

For Legal and Safety Reasons

We may disclose information if we believe it is reasonably necessary to:

- Comply with applicable law, regulation, subpoena, court order, or legal process
- Respond to lawful requests from public authorities
- Enforce our Terms of Service
- Investigate fraud, theft, abuse, misuse, unauthorized access, or security issues
- Protect the rights, property, or safety of ServiceLine, users, service providers, or others
- Resolve disputes between users
- Prevent harm, fraud, illegal activity, or security threats

Business Transfers

If we are involved in a merger, acquisition, financing, reorganization, bankruptcy, sale of assets, or similar business transaction, your information may be transferred as part of that transaction.

4. Payments, Stripe, and Financial Data

Payments through the Service are handled by Stripe. We do not control Stripe's independent privacy practices.

Depending on how you use the Service, Stripe may collect information such as:

- Name
- Email address
- Billing address

- Payment method information
- Card information
- Bank account or payout information
- Transaction history
- Identity verification information
- Government-issued identification
- Selfie or biometric verification information
- Tax information
- Fraud prevention and risk signals

If you are a customer, Stripe may collect and process payment information to complete your purchase.

If you are a stringer receiving payouts, Stripe may require additional information to verify your identity, comply with tax rules, prevent fraud, and process payouts.

We may receive or store limited Stripe-related identifiers and transaction records, such as:

- Stripe Customer ID
- Stripe Connect account ID
- Payment Intent ID
- Transfer ID
- Fee breakdown
- Payment status
- Refund status
- Dispute status
- Transaction timestamps

We do not store full card numbers, CVV codes, full bank account numbers, or full identity verification documents on our own servers.

5. Google Firebase, App Infrastructure, and Storage

We use Google Firebase to help operate, secure, store, analyze, and improve the Service.

Firebase services we may use include:

- Firebase Authentication
- Firestore
- Firebase Storage
- Firebase Cloud Messaging
- Firebase Crashlytics
- Firebase Analytics
- Remote Config
- Cloud Run

- Firebase security rules
- Related Google Cloud or Firebase infrastructure

Depending on how you use the Service, Firebase may process information such as:

- Name
- Email address
- Phone number
- Firebase UID
- Profile photo
- Account information
- Customer or stringer profile information
- Zip code
- Approximate location
- Stringer service area
- GeoFire location data
- Messages
- Images
- Reviews
- Order details
- Notification tokens
- App instance ID
- Screen views
- Custom analytics events
- User type
- Crash logs
- Device model
- OS version
- App version
- Stack traces
- Custom diagnostic keys
- IP address at the network layer
- Security logs
- Other information necessary to provide, secure, and improve the Service

We may use Firebase to:

- Authenticate users
- Store user profiles and user-generated content
- Store and retrieve text, images, messages, reviews, and order information
- Store waitlist information
- Send push notifications and app messages
- Analyze app usage and product interactions
- Diagnose crashes, bugs, and performance issues
- Configure app behavior

- Run backend infrastructure
- Enforce security rules and access controls
- Detect and prevent unauthorized access, misuse, abuse, fraud, or technical issues

6. Location Information

Our Service may require access to your location or location-related information to help users find nearby customers or stringers.

We may collect location information when:

- You create or update an account
- You enter a zip code
- You open or use the app
- You search for nearby users or services
- You request or provide a service
- You enable location-based features
- The app needs to update availability, proximity, or service area information

For customers, we may use zip code or approximate location to match you with nearby stringers.

For stringers, we may use service area information, latitude and longitude, radius, and GeoFire data in Firestore to determine where services are offered.

We do not sell precise location information. However, location-related information may be shared with other users when necessary to provide the Service, such as helping a customer and stringer coordinate a nearby service.

You may disable location permissions through your device settings. However, disabling location access may limit or prevent use of important app features.

7. Reviews, Ratings, Profiles, and Public Information

The Service may allow users to post or display reviews, ratings, comments, profile details, photos, service areas, descriptions, or other content.

Information you choose to make public or visible within the Service may be seen by other users. This may include:

- Name or username
- Profile photo
- Profile description
- Ratings

- Reviews
- General location or service area
- Services offered
- User-generated content

Please do not post sensitive personal information in reviews, messages, profile descriptions, or public areas of the Service.

8. Communications, Messages, and Notifications

The Service may allow customers and stringers to communicate with each other through in-app messaging.

We may collect and store:

- Message content
- Sender and recipient information
- Message timestamps
- Firestore message records
- Push notification tokens
- Notification delivery information.

We may use Firebase Cloud Messaging, Apple Push Notification Service, and other providers to send push notifications, booking updates, reminders, service alerts, security notices, and other app-related messages.

You can control push notifications through your device settings. However, disabling notifications may prevent you from receiving important booking, payment, security, or service updates.

9. Cookies, SDKs, and Tracking Technologies

We may use cookies, pixels, software development kits, local storage, device identifiers, attribution tools, analytics tools, and similar technologies to:

- Keep you logged in
- Remember preferences
- Authenticate accounts
- Analyze app usage
- Improve performance
- Send and manage push notifications
- Detect fraud, abuse, unauthorized access, or security issues
- Diagnose crashes, bugs, and technical problems
- Measure marketing effectiveness
- Understand app installs and attribution

Because the Service includes a mobile application and website, we may use third-party SDKs and tools, including Firebase SDKs, Apple tools, Stripe tools, HubSpot tools, and Vercel hosting infrastructure.

You may be able to control cookies, tracking preferences, app permissions, analytics settings, and notifications through your browser, device settings, or app settings. Disabling these features may affect how the Service works.

10. Analytics, Attribution, and Marketing

We may use analytics and attribution tools to understand how users find and use the Service.

This may include:

- Firebase Analytics
- Google Analytics for Firebase
- Apple Search Ads attribution
- App Store Connect analytics
- HubSpot, if connected
- Other analytics or marketing tools

We may collect or process information such as:

- App instance ID
- Screen views
- Custom app events
- Sign-up events
- Login events
- Begin checkout events
- Order submitted events
- Review submitted events
- Message sent events
- User type
- Install attribution information
- Waitlist role
- Marketing email engagement, if applicable

We may use this information for app functionality, analytics, product improvement, product personalization, and our own developer advertising or marketing.

We do not sell personal information in the traditional sense. If our use of analytics, advertising, or marketing tools is considered a “sale” or “sharing” under applicable privacy laws, we will provide any required notice or opt-out mechanism.

11. Apple App Privacy Disclosures

Apple requires app developers to disclose certain data collection and use practices in App Store Connect.

Depending on how the Service is configured and used, our Apple App Privacy disclosures may include categories such as:

- Contact Info, including name, email address, phone number, and physical address where applicable
- Financial Info, including payment information and other financial information
- Location, including precise location or coarse location
- Sensitive Info, including government-issued identification processed by Stripe Identity for stringer verification
- Identifiers, including user ID, Firebase UID, device ID, and app instance ID
- Usage Data, including product interaction, screen views, app events, and advertising or attribution data
- Diagnostics, including crash data, performance data, device model, OS version, app version, stack traces, and related diagnostic information

These categories may be used for purposes such as:

- App functionality
- Analytics
- Product personalization
- Developer advertising or marketing
- Fraud prevention
- Security
- Legal compliance

Some information may be linked to your identity depending on the data type, the purpose of collection, and how it is stored or processed.

12. Data Retention

We keep personal information for as long as reasonably necessary to provide the Service, comply with legal obligations, resolve disputes, enforce agreements, prevent fraud, and maintain business records.

For example, we may retain:

- Account records
- Order records
- Transaction records

- Payment-related identifiers
- Tax-related records
- Dispute records
- Support records
- Security logs
- App activity records
- Messages
- Reviews
- Profile information
- Waitlist information
- Marketing records, where permitted

We may also retain certain transaction, payment, tax, dispute, accounting, and identity-related records as required or permitted by law.

When information is no longer needed, we may delete, anonymize, or securely retain it as required or permitted by law.

13. Data Security

We use reasonable administrative, technical, and organizational measures to protect personal information.

We may use Firebase security rules, authentication tools, access controls, monitoring, crash reporting, security logs, and other safeguards to help protect stored information, user-generated content, messages, images, and app data.

We may also rely on security measures provided by Stripe, Google Firebase, Apple, HubSpot, Vercel, and other service providers.

However, no system is completely secure. We cannot guarantee that unauthorized access, hacking, data loss, misuse, or other security incidents will never occur.

You are responsible for keeping your account login credentials secure and for notifying us if you believe your account has been compromised.

14. Your Privacy Rights

Depending on where you live, you may have rights regarding your personal information, including the right to:

- Access the personal information we have about you
- Request correction of inaccurate information
- Request deletion of certain information

- Request a copy of your information
- Opt out of certain processing, sales, sharing, or marketing communications where applicable
- Limit certain uses of sensitive personal information where applicable
- Withdraw consent where processing is based on consent

To make a privacy request, contact us at:

contact@servicelinellc.com

We may need to verify your identity before fulfilling your request. We may also retain certain information as required or permitted by law, including records needed for security, fraud prevention, dispute resolution, tax, accounting, legal compliance, or enforcement of our agreements.

15. California Privacy Rights

If you are a California resident, you may have additional rights under California privacy laws.

These may include:

- The right to know what personal information we collect, use, disclose, sell, or share
- The right to request deletion of personal information
- The right to request correction of inaccurate personal information
- The right to opt out of certain sales or sharing of personal information
- The right to limit certain uses or disclosures of sensitive personal information
- The right not to be discriminated against for exercising privacy rights

We do not sell personal information in the traditional sense. If we use advertising, analytics, attribution, or marketing tools that are considered a “sale” or “sharing” under California law, we will provide any required opt-out mechanism.

16. Children’s Privacy

The Service is not intended for children under the age of 13, or under the minimum age required by applicable law.

We do not knowingly collect personal information from children without appropriate consent. If we learn that we have collected personal information from a child without appropriate consent, we will take steps to delete it.

Users who are old enough to use the Service but are still minors should use the Service only with the involvement and consent of a parent or legal guardian where required by law.

17. International Users

If you access the Service from outside the United States, your information may be transferred to, stored in, or processed in the United States or other countries where we or our service providers operate.

Data protection laws in those countries may differ from the laws in your country.

By using the Service, you understand that your information may be transferred to and processed in the United States and other countries.

18. Marketing and Service Communications

We may send you promotional emails, texts, push notifications, in-app messages, or other communications if permitted by law.

We may use Firebase, Apple services, HubSpot, or other service providers to send push notifications, in-app messages, booking updates, reminders, service alerts, security notices, marketing messages, and app-related communications.

You can opt out of marketing emails by following the unsubscribe instructions in the email. You may control push notifications through your device settings.

Even if you opt out of marketing messages, we may still send transactional or service-related communications, such as payment confirmations, booking updates, account notices, security alerts, support messages, and legal notices.

19. Third-Party Links and Services

The Service may contain links to third-party websites, services, or integrations.

We use third-party services to help provide payments, hosting, storage, analytics, notifications, security, messaging, identity verification, marketing, and app functionality.

Third-party services we use or may use include:

- Google Firebase, including Firebase Authentication, Firestore, Firebase Storage, Firebase Cloud Messaging, Firebase Crashlytics, Firebase Analytics, Remote Config, and Cloud Run
- Stripe, including Payments, Connect, and Identity
- Apple, including Apple Search Ads attribution, App Store Connect analytics, and Apple Push Notification Service
- HubSpot, for waitlist marketing and contact management if connected
- Vercel, for website hosting

These third parties may process information as described in this Privacy Policy and in their own privacy policies or legal terms.

We are not responsible for the privacy practices, content, or policies of third parties. Your use of third-party services may be subject to their own terms and privacy policies.

Third-party privacy policies include:

- Google Firebase: <https://firebase.google.com/support/privacy>
- Google Privacy Policy: <https://policies.google.com/privacy>
- Stripe Privacy Policy: <https://stripe.com/privacy>
- Apple Privacy Policy: <https://www.apple.com/legal/privacy/>
- HubSpot Privacy Policy: <https://legal.hubspot.com/privacy-policy>
- Vercel Privacy Policy: <https://vercel.com/legal/privacy-policy>

20. Changes to This Privacy Policy

We may update this Privacy Policy from time to time.

If we make material changes, we may notify you by email, in-app notice, website notice, or by updating the effective date above.

Your continued use of the Service after an updated Privacy Policy becomes effective means you accept the updated policy.

21. Contact Us

If you have questions about this Privacy Policy or our privacy practices, contact us at:

StringinLLC

Email: contact@servicelinellc.com

Address: [Insert business mailing address, registered agent address, or other appropriate contact address]