billfixers

January 2021

Security & Data Overview

BillFixers deals with sensitive PII and other data. As a consumer advocate, we're committed to user privacy and security. We work to accomplish that goal through data minimization, access limitation, encryption, best in class vendors, and additional security practices.

PERSONAL DATA

What personal data does BillFixers hold?

In order to negotiate bills on behalf of users, we need to have access to the same data that vendors require for over-the-phone authentication.

Name
Email Address
Bill Statements
- **Bill Account Number**
- **Address**

Phone Number
Service/Pricing Details
Last 4 of SSN*
Account PIN/Passcode*
Security Answers*

*We work to hold only the relevant data for a particular negotiation. For example, providers are coded so that we only request the last four of a user's SSN if it is necessary to negotiate with that particular provider.

We generate additional data through our negotiations and support processes, such as service and pricing information from vendors, limited billing details, and support correspondence. We hold temporary logs of IP addresses for logging/monitoring security purposes. If users choose to connect via Plaid, we also store transaction history.

We do not store full socials, credit card numbers, or online passwords as part of our process.

KEY TAKEAWAYS

Data Encryption

Data is AES-256 encrypted at rest and in transit.

No Selling/Sharing

We do not sell or share personal data.

Log & Monitor

We log activities and errors and review odd behavior.

Data Minimization

We request and store the minimum relevant data.

Access Limitation

We restrict customer, employee, and API access permissions to only the necessary data.

Secure Vendors

We use best in class, security certified vendors to handle sensitive data.

billfixers

DATA STORAGE

How is data stored and protected?

We rely on cloud services providers and do not do any on site storage. **All data is encrypted at rest and in transit.**

Bill Statements

Bill statements, generally either PDFs or JPG/PNG photos of bills, are stored AES-256 encrypted in **Amazon Web Services S3 Storage**. Paper statements mailed physically to our office are scanned and moved to S3, then the hard copy is shredded. Access is available to employees only through unique, randomly generated links that expire and re-generate every five minutes.

Database & App

Our app and databases run on **Heroku**'s latest heroku-20 stack, where data is also stored at rest with AES-256 encryption. We also force TLS/SSL for any internal or external access to our app, so data is encrypted in flight regardless of whether its being accessed by a customer, a partner via API, or by ourselves internally. We use **Lockbox** for an additional layer of application-level AES-GCM encryption on the most sensitive information, like bill PINs or the last four digits of a user's SSN.

3rd Party Vendors

We rely on third parties for services like support and billing. These providers store data as well. Payment processing is handled by **Stripe**, a PCI Compliance Level 1 vendor. Support is handled with **Freshworks**, which is SOC 2 certified. Internal communications are on **Slack**, also SOC 2 certified. We are beta-testing **Plaid,** the industry standard for pulling transactions and plan to scrub any irrelevant data.

We follow security best practices such as the Principle of Least Privilege and Multi-Factor Authentication for our own access to third party vendors.

Who has access to data?

We do not sell or share personal data. There are three groups who have access to individual parts of a user's data: the user themself, a partner if the bill was created via API, and BillFixers employees. **Each role has limiting access privileges**. For example, a user or partner can submit a PIN for a bill, but not view it after creation. An employee with standard permissions could view the bill they're working on, but not larger reporting on bills. Employees may only access data on password-protected devices.

billfixers

ADDITIONAL SECURITY

What other ways does BillFixers keep user data secure?

Data security is necessarily an ongoing project. We continually try to review and improve our practices. We are always looking for feedback from users, employees, partners, and others to add or improve our measures to protect our users' data. Here are some of the things we do right now:

PREVENTATIVE

Sanitized Inputs

All customer-facing inputs are sanitized to prevent code injections.

Error Track & Patch

All application errors are logged in **Sentry**, then reviewed, and patched.

Password Policies

Passwords must meet security requirements and employees reset annually.

Dependency Security

Dependabot by **GitHub** is used to monitor for security alerts and update regularly.

Secure Communication

Internal communication happens over **Slack**, preventing email phishing.

Employee NDAs

All employees must sign a Non-Disclosure Agreement encompassing user data.

Bad Actor Prevention

DDoS attacks and other suspicious traffic are prevented by **Cloudflare.**

Responsible DIsclosure

We have a dedicated email for vulnerability disclosures and prompt for bug details.

Physical Security

Our office is locked, locks changed regularly, and keyholder access limited.

DETECTIVE

Monitoring

Sanitized external traffic is monitored via **LogRocket.** Data is scrubbed monthly.

Data Change Logs

When a user or employee edits the data on a user's bill, the change is logged.

Physical Security

Entrances and exits at our office have security cameras monitoring them.

billfixers

API SECURITY

How do we handle security and data in our API?

BillFixers offers a GraphQL API to partners so that they can offer bill negotiation to their users in their own apps or platforms. Doing this necessitates sharing information between partners and BillFixers. Partners are relying on us to maintain the standards of trust and security their own users expect in their relationships, so privacy and security is a priority.

Who has API Access?

Our API and its documentation are private. Access has to be personally generated by one of four people who hold the highest level Admin privileges in our system.

In order to read or write via API, you need to pass a personalized email address and randomized token with each request. Access is based around user accounts, which are connected to partner accounts, so any successful API access is attributable not just to a specific partner, but to a specific person's key. An attempt to access the API without a valid user account and token will give a generic error and log the attempt.

What can they access?

Partners with API access can review the list of providers we negotiate, create customers and bills, and they can access **specific information about only those customers and bills that they have created.** The API can also be used to read requests from us for additional information or consent and write responses to them. Finally, it can be used to see the status of the negotiation and details of the savings themselves once negotiation finishes.

For security reasons, **API read/write access is not symmetrical.** For example, while you can send the answer to a security question over the API, you cannot retrieve answers to security questions.

We also offer the optional use of Webhooks. Webhooks events do not contain any personal information, just two items: an event type and an item ID. All objects interacted with via the API have a randomly generated unique API ID, separate from our internal item IDs. Here's an example of a Webhook:

```
{
  "event_type": "customer.created",
  "id": "customer_5e12133055ada65444775e2f0bf7484f"
}
```