How payment information is protected

An overview of how credit/debit card and bank account details are kept safe.

Written by Wes Cossick
Updated over a week ago

Any time credit card, debit card, or bank account details are provided on our platform, this information is sent directly from the user to Stripe using an encrypted connection (HTTPS). These details never touch our servers, and we cannot access sensitive details after they're sent to Stripe.

Who is Stripe?

They're the company that processes payments for Google, Microsoft, Amazon, Salesforce, Uber, Expedia, Spotify, and millions of other companies across the globe. Stripe is the definitive leader in payment processing, having processed payments for more than 90% of U.S. adults.

Stripe has been audited by a PCI-certified auditor and is certified to PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry. For more technical details about Stripe's security, see: https://stripe.com/docs/security/stripe.

How we keep data safe and secure

An outline of the many security measures in place.

Written by Wes Cossick
Updated over a week ago

Security is always one of our highest priorities. We know that thousands of communities count on us to keep their member information, files, and private content secure. That's a responsibility we don't take lightly.

As a result, we've employed many techniques that meet or exceed industry standards, including quite a few measures used for bank-level security. We'll summarize some of them below, by technique.

HTTPS

We encrypt all traffic to our community websites with HTTPS, a crucial measure that prevents many common forms of stolen data. Although others charge extra or overlook this necessity entirely, we enable HTTPS completely free for every community website. We go into more detail about this security feature in this help article about our use of HTTPS.

HSTS

We enable HSTS on all community websites. It's a modern security technique that protects against even highly sophisticated attempts to steal data from your users, by requiring browsers to always use HTTPS for connections to your website.

Data encryption

Behind the scenes, in our data storage systems, we encrypt important personal data. This means that if it's ever intercepted or falls into the wrong hands, it will be useless without the means to decrypt it.

Data hashing

Data hashing is like encryption, except it's one-way. We use this primarily for passwords, secrets, and certain API keys. That means that if hashed data falls into the wrong hands, it's impossible to convert back into its original form.

Login techniques

Our authentication system uses a variety of account protection techniques, including (but not limited to) account locking mechanisms, aggressive API key expiration, multiple bruteforce countermeasures, and stolen account detection. These details are relatively technical, but you can be confident we do everything possible on our end to keep your member information safe.

Password strength

Many companies require users to simply meet a list of requirements for passwords... some number of uppercase/lowercase letters, numbers, special characters, etc. While this simple method can help nudge people toward more secure passwords, it's also a vulnerable technique. We don't take shortcuts when it comes to security, so we calculate the mathematical entropy of passwords and require that to meet a secure threshold. This calculation is a true measure of how difficult the password is to crack and isn't susceptible to permitting insecure passwords.

Additionally, we places no limits on how long a password can be or what characters it can use. These types of limits serve only to reduce the strength of passwords.

Email scraping protection

We employ multiple layers of cutting-edge email scraping counter measures. These serve to protect published email addresses from falling into the hands of bots, scammers, and spammers.

Email spoofing prevention

We implement strict SPF policies and strong DKIM records for our company domain and every community website domain to prevent email addresses from being spoofed. In other words, you can be confident that emails that come from **@hoa-express.com** or ***@yourcommunity.com*** were not sent by spammers.

Form security

We protect publicly available contact forms from bot submissions by utilizing a number of intelligent detection mechanisms.

Automated testing

We run automated tests before deploying any change to make sure all our security features work exactly as intended. This allows us to confidently make improvements to our system without worrying about accidentally breaking a security feature.

Secure workflows

Our product team has designed highly secure workflows to ensure user details, infrastructure secrets, and other sensitive information remains safe. This includes limiting which team members have access to private information and keeping secrets from being handled by unnecessary third parties, among many other techniques.

Security conscious vendor selection

We only work with companies that care as much about security as we do. We'll never utilize companies who do not maintain excellent reputations.

Content restriction settings

An important form of data security is controlling who can see content, and who cannot. Our interface gives administrators the ability to set detailed content restrictions. Limit pages and files to:

- just approved accounts
- just certain account types
- just a custom group of members
- just one or two specific people
- not one or two specific people

...you can see where this is going—the options are limitless. On top of that, we've built in considerable security measures to make sure that the chosen restrictions are enforced.

Privacy preferences

Members can choose their own privacy preferences, allowing them to control what information other members and visitors see on the website. For instance, they can hide information from the community directory if preferred. They can also choose what contact information is displayed if they're a leader within the community and what information remains private.

Backing up data

This security measure doesn't have to do with protecting you from stolen data; rather, it protects your community from lost data. We back up all data (including members, pages, files, and much, much more) on a regular basis throughout the day. Learn more by reading our help article about how we keep your data safe from loss or corruption.

So much more

While this list seems extensive, it's only a partial list of the ways we keep your data safe and secure at HOA Express. If you ever have or discover a security concern though, please immediately contact our customer success team and we'll quickly handle the matter.