SECURITY WHITE PAPER

ChangeMaker Initiative by Hello Donor

Document Date: June 2021

HELLO DONOR, INC.
10 Roswell Street, Suite 101, Alpharetta, GA 30009
Phone: 678.240.1035 | Web: hellodonor.com
Email: info@hellodonor.com

hellodonor

INTRODUCTION

Hello Donor's mission is to financially equip schools and nonprofits to fulfill their mission and inspire supporters and future generations to give on a recurring basis.

We make fundraising easy, fun, and safe with recurring donations with change round-up. We believe that we need to make your data secure, and that protecting it is one of our most important responsibilities. We're committed to being transparent about our security practices and helping you understand our approach.

The focus of Hello Donor's security program is to prevent unauthorized access to customer data. To this end, our team of dedicated developers, working in partnership with top financial partners, take exhaustive steps to identify and mitigate risks, implement best practices, and constantly develop ways to improve.

OUR COMMITMENT TO YOU

- ☑ We do NOT access, store, or record the donor's credit card, debit card, confidential, and/or financial information. We leave that to our industry-leading partners.
- ☑ We do NOT sell or share your financial information with outside companies. Hello Donor will never share your data without your permission.
- ☑ We provide the highest level of security and availability within our means. To accomplish this, we use the best-in-class security tools and practices to maintain a high level of security.
- ☑ Your financial data is secure. Our financial partner that processes all of Hello Donor card transactions 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.

INDUSTRY-LEADING FINANCIAL PARTNERS

Hello Donor contracts with best-in-class third-party credit/debit card professionals who continually perform penetration tests, vulnerability assessments, and source code analysis to validate the security of Hello Donor's card processing functions. Our engagements cover the full spectrum of application architecture, role-based security, data stewardship, and application functionality.

Our technology partners:

- **Stripe** - If you have ever used a debit or credit card to buy something at Target or on Amazon, the payment processing of your transaction was handled by Stripe. Stripe is the leading technology for the economic infrastructure of the Internet. They are the payment processing component that supports Hello Donor, as well as millions of small businesses and publicly traded companies. They have a robust platform that allows companies, like Hello Donor, to integrate with their systems and benefit from their industry-leading security. Stripe maintains the strictest levels of PII Compliance.

- **Plaid** - Plaid is owned by Visa. They secure financial institutions like your local and global bank accounts. Over 4,500 companies trust Plaid to connect their financial institutions to their applications. When you sign up for change round-up, our system needs to calculate how much change should be donated to the organization you are supporting. When you authorize change round-up, our partner Plaid, will pull your transaction data needed to calculate your change. If you have used Venmo, Acorns, or any other technology that syncs with your bank account, you have experienced the benefits of Plaid. Plaid has analyzed over 10 billion transactions.

- **Amazon Web Services (AWS)** – AWS hosts applications that Hello Donor operates. AWS is the world's largest provider of computing services available on the Web, from globally distributed servers to highly automated data centers. AWS is vigilant about your privacy. All data flowing across the AWS global network that interconnects their datacenters and regions is automatically encrypted at the physical layer before it leaves their secured facilities.

SECURITY DETAILS

STRIPE

HTTPS and HSTS for secure connections

Stripe forces HTTPS for all services using TLS (SSL).

- Stripe.js is served only over TLS
- Stripe's official libraries connect to Stripe's servers over TLS and verify TLS certificates on each connection

We regularly audit the details of our implementation, including the certificates we serve, the certificate authorities we use, and the ciphers we support. We use HSTS to ensure that browsers interact with Stripe only over HTTPS. Stripe is also on the HSTS preloaded lists for both Google Chrome and Mozilla Firefox.

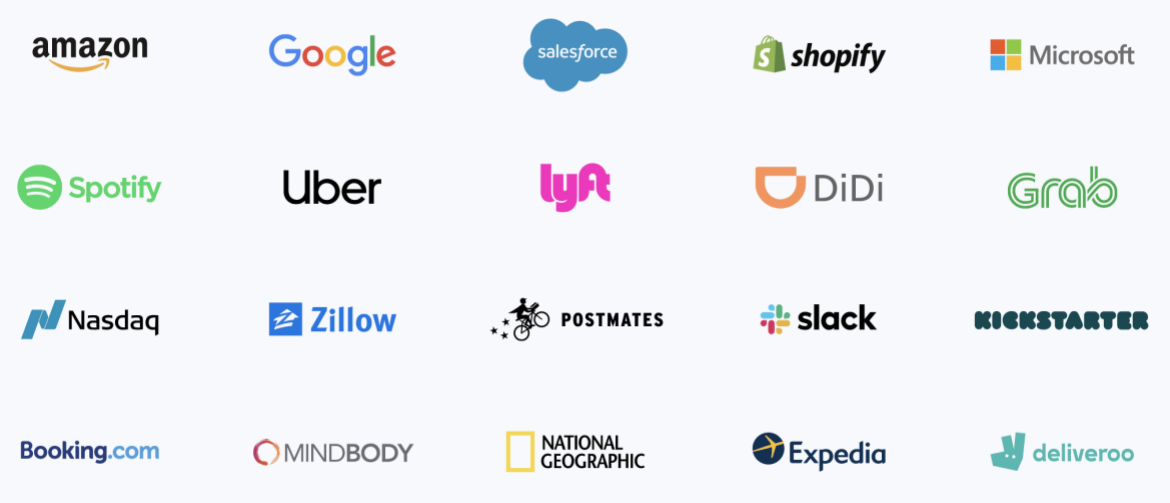
Encryption of sensitive data and communication

All card numbers are encrypted at rest with AES-256. Decryption keys are stored on separate machines. None of Stripe's internal servers and daemons can obtain plaintext card numbers but can request that cards are sent to a service provider on a static allowlist. Stripe's infrastructure for storing, decrypting, and transmitting card numbers runs in a separate hosting environment, and doesn't share any credentials with Stripe's primary services (API, website, etc.).

PCI compliance and secure communications

Anyone involved with the processing, transmission, or storage of card data must comply with the Payment Card Industry Data Security Standards (PCI DSS). Stripe has been audited by an independent PCI Qualified Security Assessor (QSA) and is certified as a PCI Level 1 Service Provider. This is the most stringent level of certification available in the payments industry.

Partial list of Stripe clients:



PLAID

Encryption safeguards your data while using Plaid

When you use Plaid to connect a bank account to an app, we help keep your data safe and private with best-in-class encryption protocols like the Advanced Encryption Standard (AES 256) and Transport Layer Security (TLS).

Multi-factor authentication

To help ensure a secure account connection, Plaid built its own multi-factor authentication (MFA) in case your financial institution doesn't offer one. With Plaid's MFA as a backup, almost all logins feature this extra security step.

Built on secure cloud infrastructure

We use modern cloud technologies to host the Plaid API. By using cloud infrastructure, we're able to leverage years of safety enhancements to better protect data.

Around-the-clock monitoring protects information

Robust safety monitoring, automated alerts, and a 24/7 on-call team helps Plaid quickly respond to and resolve any potential issues, so you can be confident your private information is secure.

Independent security testing

Some of the most trusted security researchers, app developers, and financial institutions regularly audit Plaid's API and security controls. And our bug bounty program makes sure anyone, anywhere can help make our systems safe.

Creating a safer financial future for everyone

We share our security practices and technologies to make sure we're moving toward a more secure digital financial ecosystem together. And we continuously work with fintech companies and banks to push the entire industry forward.

PLAID

1 in 4

1 in 4 US adults has connected a financial account to an app with Plaid—and that number is growing every day.

You're in good hands

At Plaid, our business model—and our reputation—depend on keeping your data safe. That means working around the clock to help keep your data secure.

>4,000

There are more than 4,000 financial apps and services that are powered by Plaid.

>11,000

Plaid connects to over 11,000 US financial institutions, as well as many more in Canada, the UK, and the European Union.

AMAZON WEB SERVICES (AWS)

Distributed infrastructure

Hello Donor utilizes services deployed by AWS to distribute production operations across multiple physical locations. This distributed topography from AWS protects Hello Donor's service from loss of connectivity, power infrastructure, and other common location-specific failures. Production transactions are replicated among these discrete operating environments to protect the availability of Hello Donor's service in the event of a location-specific catastrophic event. Hello Donor also retains a full backup copy of production data in a remote location significantly distant from the location of the primary operating environment.

Data protection

AWS provides services that help you protect data, accounts, and workloads from unauthorized access. AWS data protection services provide encryption and key management and threat detection that continuously monitors and protects your accounts and workloads.

Identity & access management

AWS Identity Services securely manage identities, resources, and permissions at scale. With AWS, identity services for our workforce and customer-facing applications manage access to our workloads and applications.

Network & application protection

Network and application protection services enable enforcement of fine-grained security policy at network control points across our organization. AWS services inspect and filter traffic to prevent unauthorized resource access at the host, network, and application-level boundaries.

Compliance & data privacy

AWS provides a comprehensive view of our compliance status and continuously monitors our environment using automated compliance checks based on the AWS best practices and industry standards.

CONCLUSION

We have an existential interest in protecting your data. Every person, team, and organization deserve and expect their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we continue to work hard to maintain that trust.

Please contact us at info@hellodonor if you have any questions or concerns.

Hello Donor. The future in fundraising.