

CASE STUDY

JustGiving payments and donor privacy

As one of the world's largest online social platforms for charitable giving, JustGiving needed to comply with strict regulations from the Payment Card Industry Data Security Standard (PCI DSS) about the handling of sensitive donor information and donor payment card data. The merchant potentially faced a series of very large, escalating fines for non-compliance.

The PCI DSS provides a set of requirements to ensure that sensitive data is protected by merchants like JustGiving. According to PCI DSS compliance regulations, every organization that processes, stores, or transmits payment card data needs to maintain a secure environment.

JustGiving has helped donors raise over \$4.5 billion since they were founded and handles credit card information for over 24 million users with about 10 million transactions each year. However, charitable giving can reveal much about a donor – including personal details relating to health, as well as valuable financial data. Therefore, private information shared with charitable organizations needs to be protected.

Solution

JustGiving chose the Protegrity Privacy Protect solution with its patented vaultless tokenization technology because they determined that was the best way to protect donor payment card data and reduce cost, time, and complexity of PCI DSS audits.

Rather than encrypting data, tokenization replaces sensitive data with random data of the same type and length. Because there is no mathematical relationship to the original data, tokenized data is considered replaced or removed, and therefore secure. Systems that only process tokens are exempt from the PCI DSS audit scope.

The Protegrity Privacy Protect solution included a Protection Server and Enterprise Security Administrator for centralized oversight and administration of secure data across the entire organization.

Initially, JustGiving evaluated no-cost solutions from their payment service provider as well as a solution from another vendor but only Protegrity offered the security, flexibility, and control that the merchant needed.

While payment processors offer some protection to their customers using payment tokens, this approach does not protect sensitive donor information that is separate from the payment data.

Depending on the number of payment processors used and the variety of donation sources, the complexity of managing a database of payment tokens for donor information also creates more problems than it solves. Making the organization reliant upon the processors for protection can also limit them to those payment processors.

Impact

Utilizing Protegrity's vaultless tokenization solution enabled JustGiving to satisfy PCI DSS compliance while allowing full control over the data and privacy protection for the individual donors.

Having internal control of data security enables customized protection with maximum performance and rapid response times. It also allows JustGiving to more easily adapt to future changes, including updates to PCI DSS, privacy and data residency laws, and new platforms and payment methods.

Protegrity enables us to realize our ambitions to provide peace of mind for donors without compromising the margins of their investment, in a fraction of the time it would have taken to build a solution ourselves.

– Richard Atkinson,
former CIO, JustGiving

Key Highlights

Industry

Charitable Giving

Challenge

Protect donor privacy and payment card information to meet PCI DSS requirements while maintaining full control of the data and flexibility to use it for future initiatives.

Solution

Deployed Protegrity *Privacy Protect* with vaultless tokenization for fine-grained protection of sensitive PCI data.

Impact

Met donor privacy and PCI DSS requirements for over 24 million users and 10 million transactions per year, reduced the cost, time, and complexity of PCI DSS audits, and enabled flexibility for future payment methods.

Objectives

- Protect their donor database to build trust and allow people to easily find and connect with the causes they care about.
- Comply with PCI DSS regulations to securely protect payment card data for over 24 million users and 10 million transactions each year.
- Provide centralized oversight and administration of secure data across the entire organization.
- Reduce the cost, time, and complexity of annual PCI DSS compliance audits.
- Provide enough flexibility to use secure data for future initiatives.

Challenges

- Huge volumes of personal donor data.
- Slim profit margins from charitable giving do not leave much room to spend money on security, making it a delicate balancing act to spend as little as possible but also protect sensitive data with strong technology.

FOR MORE INFORMATION, VISIT WWW.PROTEGRITY.COM

What is Privacy Protect?

Privacy Protect empowers businesses to extract value from sensitive data while ensuring the privacy of customers and employees is preserved. We understand that different industries have different standards, while local cultures, customs and laws also have varying requirements for data ownership, sharing and privacy.

By evolving with regulations, like PCI DSS, GDPR, CCPA, GLBA, HIPAA and so many others, Privacy Protect continuously helps organizations make the most of their data while staying in step with compliance now and in the future.

Privacy Protect for Organizations

- Future-Proofs Against Evolving Regulations
- Simplifies Data Security Management and Protection
- Facilitates Access to Sensitive Data
- Promotes a Mature Data-Privacy Practice
- Protects Retailers from Costly Data Breaches

Share the data across borders with those who need it and protect it against those who don't.



Business Value

- *Privacy Protect* is good for JustGiving because it enabled them to securely protect sensitive donor information and payment data.
- Protegrity's tokenization reduced the time, money, and complexity of the required annual PCI DSS audits.
- Customized protection enabled flexibility, allowing JustGiving to more easily adapt to future payment methods.

Technical Value

- The unique architecture of Protegrity's vaultless tokenization technology provides all the benefits of tokenization without the drawbacks and limitations of traditional tokenization; no ever-growing token lookup tables and no replication, which can seriously affect performance, and most importantly, no stored sensitive data.
- Protegrity's centralized policy, key management, auditing, and reporting allow JustGiving to centrally manage the security of sensitive data, regardless of where it goes.
- With built-in separation of duties, it increases security, compliance, corporate oversight.

Why Protegrity?

For more than two decades, Protegrity, a global leader in data security, has protected the sensitive data of the largest brands in the world, including four of the world's 15 largest banks and three of the world's leading multinational companies.

Protegrity provides the only platform that lets enterprises decide which data should be classified as sensitive and allows them to control how they safeguard that data, enabling the bank to securely and compliantly leverage external cloud data analytics.

With Protegrity, this international bank has unrestricted enterprise access to all generally available data security technology, both now and in the future, including advisory services and 24 x 7 support.

FOR MORE INFORMATION, VISIT WWW.PROTEGRITY.COM