comforte

CASE STUDY

ONE OF THE WORLD’S LARGEST FASHION RETAILERS CHOOSES TOKENIZATION

Encryption is an effective and secure method for protecting data, especially data at rest. In highvolume, real-time payment environments, tokenization is the data protection method of choice for many major retailers, banks, and credit card companies around the world because it offers top of the line protection with minimal impact on processing speed. A high-profile fashion retailer chose comforte’s easy-to-implement tokenization solution to add an extra layer of protection to their payments network, while maintaining the high level of service their customers expect.

CUSTOMER PROFILE

In most retail stores, whenever a customer uses a payment card, the transaction details are stored in a central computer system to facilitate the exchange of money for the items sold. Unless the retailer outsources their payment processing to a service provider, storing transaction details is a normal business operation.

This major fashion retailer in the US is no exception. With close to 900 stores in North America, accepting payment cards has long been a staple as part of their customers’ experience: the firm has accepted payments from all major card labels (Visa, MasterCard, Amex, and Discover) along with having their own private label credit card for more than 30 years.

CHALLENGES

Stored transaction details contain payment card data along with other personally identifiable information, which is a very attractive target for hackers and other bad actors looking to steal valuable data. On the dark web and underground websites, stolen credit and debit card details are sold for large sums of money and are used to purchase illegal items and exploited for other criminal purposes. This is why hackers are incessantly trying to breach and extract valuable data from organizations of every size and from every industry. Data breaches have practically become a fact of life and sooner or later most organizations will experience at least one. Despite their strong data security stance, this highly recognized and trusted retailer was eventually breached, which prompted their data security team to take immediate action and add an additional layer of protection that would prevent similar and potentially larger breaches in the future. In light of recent events, these additional security measures were readily approved at the board level.

As part of their existing data security program, the retailer already used encryption to protect the payment card numbers, as well as a unique internal ID number associated with every payment card. One of the challenges they faced was to extend that protection to include personal information such as names, addresses, birthdates, etc. of their valued customers. While payment card numbers are an obvious target, bad actors are always looking for new ways to extract value from any kind of data they manage to gain access to. Therefore, the new solution had to make it simple to scale and extend protection to additional forms of data as new situations and changing circumstances require.

QUICK FACTS

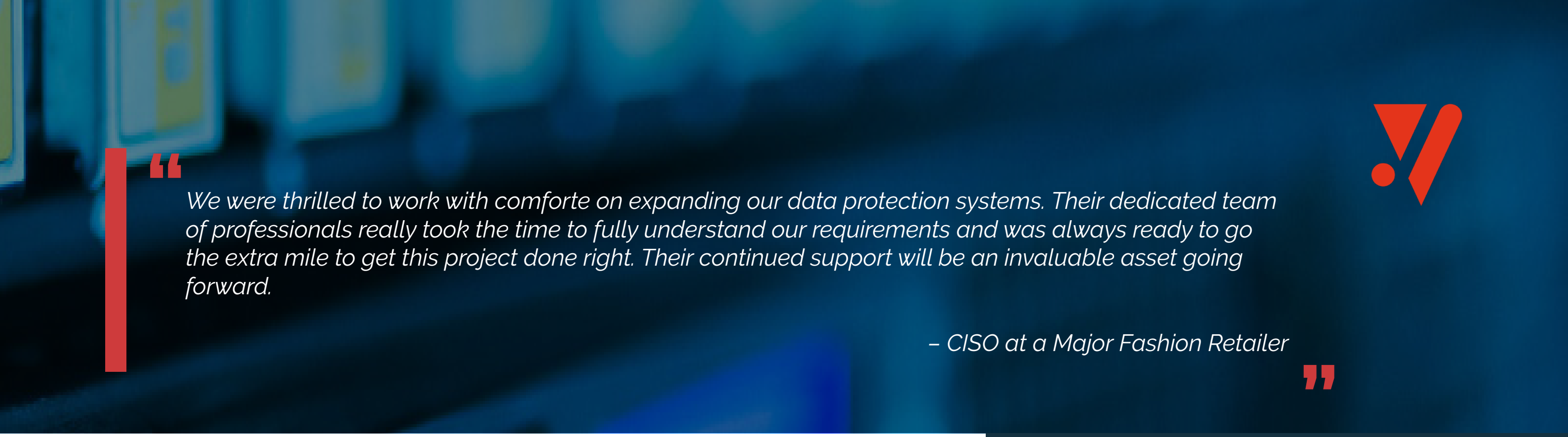
- Data protection extended beyond PANs to include personal data
- High level of security as with encryption but now with reduced burden on IT resources
- PCI audits expedited by taking sensitive data out of scope
- Encryption key management no longer required for tokenized data
- Tokenization was easily retrofitted to existing data security systems
- Scalable data protection tools will facilitate cross-regulatory compliance

SECURE YOUR GROWTH WITH COMFORTE

With more than 20 years of experience in data protection on truly mission critical systems, comforte is the perfect partner for organizations who want to protect their most valuable asset: data. comforte’s Data Protection Suite, SecurDPS, has been built from the ground up to best address data security in a world that is driven by digital business innovations, empowered customers, and continuous technology disruptions.

We are here to help secure your growth by providing expertise, an innovative technology suite, and local support.

To learn more, get in touch with a comforte representative today by visiting: **www.comforte.com/contact.**



> *We were thrilled to work with comforte on expanding our data protection systems. Their dedicated team of professionals really took the time to fully understand our requirements and was always ready to go the extra mile to get this project done right. Their continued support will be an invaluable asset going forward.*
>
> *– CISO at a Major Fashion Retailer*

Furthermore, the retailer has a very high transaction volume running on hybrid cloud infrastructure. This means that activating encryption for all customer data across their complex landscape would have added additional demand to their systems. Encryption is excellent for protecting data at rest, however, in order to use data for standard business processes, decryption needs to occur at certain stages. Encryption and decryption processes take up additional computing power and may impact transaction speed and performance. During peak times when customers visit their stores, their transaction volume may reach over 800 transactions per second collectively from all the POS devices in the stores as well as online transactions. The last thing this retailer wanted to do was risk slowing down authorizations at their point of sale as this could harm their world-renowned customer service.

Encryption and decryption also increase IT operations, specifically the management of encryption keys. As a common practice in encryption processing, encryption key management responsibilities require refreshing and replacing encryption keys every so often (also called rotating keys), as to reduce the possibility of data exposure should the encryption keys be lost or stolen. The retailer expects its volumes to grow year over year; therefore, it was natural for them to expect their operations and key management functionality to grow as well. To put this effort into perspective, based on the annual volume from this retailer, rotating encryption keys on one billion payment cards every year was not a task they wanted to continue.

SOLUTION

Tokenization

The retailer chose tokenization to secure sensitive data throughout its enterprise. Tokenization replaces sensitive data elements with a surrogate value of no exploitable value, also referred to as a token. It differs from classic encryption in that it does not require encryption keys or key management. This makes tokenization an ideal data protection method for growing organizations with high transaction volumes because without the need for key management, there is less risk of sensitive data exposure and lower operational impact since no encryption key management needs to be planned and resourced.

Format Preservation

Another major requirement was that when sensitive data is protected, it should stay in the same format so that the retailer could still use it throughout their enterprise and receive the same results. For example, tokenization replaces a 16-digit credit card number with a 16 digit token, which can be used for processing a payment without having to expose the original 16 digit number at any step of the way. The same principle can be applied to other forms of sensitive data such as names, dates of birth, phone numbers, etc. This allows the retailer to maintain data usability throughout the lifecycle of each customer, throughout their applications and services, and provide an added layer of security to stave off data exposure incidents and breaches.

Proof of Concept

The retailer performed a Proof of Concept (POC) project using the comforte tokenization solution and were very happy with the results as they were able to meet all of their requirements in terms of speed, security, and format preservation..

> *At comforte, our mission is to provide solutions to protect the data that organizations have been entrusted with. We are very excited to continue that mission by adding tokenization to this major retailer's information security tool belt and helping to keep their loyal customers' data safe.*
>
> *– Michael Deissner, CEO at comforte AG*

BENEFITS

Tokenization is recognized by the PCI Security Standards Council as a strong approach to cardholder data protection. The new tokenization has allowed the retailer to stay in compliance with PCI DSS, but now at much lower cost.

Reducing PCI Audit Scope

Two added benefits resulted from the switch to tokenization as the data protection method. First, the retailer can reduce the scope of the security audits they are subjected to each year. Typically, the security audits for PCI DSS compliance require the audit to include all systems which contain the original payment cardholder data. Since the tokenization process replaces the original data with a token, most systems can be taken out of the scope of the security audit, since the original data no longer exists. In fact, entire stores could be taken out of scope, which greatly reduced the time and cost of audits.

Cross-regulatory compliance

In addition, tokenization positions the retailer to be ready to respond to other data privacy laws surrounding the processing of personally identifiable information (PII). In the US, each state has come out with – or will be coming out with – data privacy laws that protect customer data. Based on how the retailer uses personal data from its customers, it may be subject to additional data privacy laws down the road, with different requirements. Tokenization fulfills the act of replacing sensitive data with surrogate values and if there are any new data privacy laws the retailer has to comply with in the future, extending protection to additional data is only a matter of an API call.