TOKENEX

ORVIS®

SPORTING TRADITIONS

Since 1856

The Orvis Company safeguards customer payment and personal data in a multi-channel retail empire with tokenization

Orvis Places a Premium on Protecting Customer Data

The Orvis Company is a 162-year-young outdoor retailer, adventure travel coordinator, and conservation advocate headquartered in the old New England town of Manchester, Vermont, with major operations in Roanoke, Virginia and the United Kingdom. Reflecting its New England roots and founder Charles F. Orvis, the management team places high value on customer service; integrity, mutual respect, praise and recognition of employee associates; highest quality goods and services; and sporting traditions that promote the conservation of natural resources. These core values permeate every operation at Orvis, including the information technology and data security team.

Orvis' Chief Information Security Officer Tyson Martin understands the responsibility of maintaining the trust that Orvis customers have in not only the company's many products and services, but that their personal information is safe from data breaches and theft. The ongoing reports of data breaches in the last few years and the resulting damage to brands, management, and customer trust initiated a thoughtful overhaul of the three commerce channels that were the foundation of Orvis' retail and adventure travel business. "We knew we had to securely encrypt the transactions flowing through the e-commerce, email and phone contact center, retail store and field point-of-sale channels to keep incoming payment and personal data safe," says Martin. "But we also wanted to remove all the sensitive data from our internal IT systems so that in case of a breach, there would not be any customer data to expose."

Five Principles for the Finding the Right Security Platform Partner

Martin's team began their quest in 2016 for a security platform with five principles in mind. "We created an overall strategy for what we want to do as a business. Then we wanted to find a security solution that matches key portions of that data strategy," recalls Martin. "Our expertise is retail and customer service. We don't pretend to be able to build a totally secure system on our own. That would require a huge investment in hardware, software, and people-power. It would be fiscally irresponsible to build our own secure data centers. We knew that there would be appropriate solutions already available. We just had to find the perfect fit for our organization."

Simplification was the first key principle. Martin makes the analogy of a complex machine: "If a machine needs twelve gears to work, and I bring that down to three gears, then I don't have to be quite as much of a mechanic to fix problems when they occur. Simplification is key, if you have three channels that operate differently, then that means you have three machines that can breakdown in different ways. So, we wanted the three channels to function in the same manner; to have the same mechanisms behind the scene."

The second principle was that the cost of securing the multitude of transactions resulting from having over 5,000 products with 32 million visits/year for the e-commerce site alone needed to be predictable and the billing clear and transparent. "We wanted to know that annually it will be X price, and yet have the ability to grow at a reasonable cost, and we don't have to worry about paying exorbitant fees for transaction surges during holidays, or having interchange and other hidden fees. Our cell phone bills are complicated enough. We wanted something that was much simpler than that from a billing perspective."

The third goal was to ensure that the security solution had zero impact on customer interactions or how the associates in contact centers and retail dealt with payment information. "That's a big goal because when you are a distributed organization, it can be difficult to connect with people one on

one. To walk them through and train them on new procedures. We don't want any procedures that frustrates an associate or a customer."

Forth, the security platform had to protect all customer data. "Payment card data is important, of course, but our customers are not just their credit card number. We collect email addresses, telephone numbers, mailing addresses; passport numbers and dietary information for our adventure travelers. Data that we collect today that we analyze for customer service, we don't necessarily understand the sensitivity of everything we collect because that's a moving target. So, we needed a solution that could protect any type of data. Respect for the security of customer data, whether it is payment or personal, is of utmost importance."

The fifth principle was to ensure that the resulting security platform performed as envisioned. "We made it very clear to the folks that we interviewed for this security project that we needed a clear vision of the end result. I felt that with a solution that is simple, the vendor should be able to paint a clear picture at the beginning of the end, how it would all work together and at what cost. We are a New England-based company and we have a frugal gene in us that requires we know the value we are getting for our work.

With these principles in mind, the selection of a data security platform took a few months of research and interviews of potential partners. It quickly became apparent that there were leaders and laggards. "Some vendors couldn't articulate a clear end vision of the security configuration. Others couldn't provide an accurate pricing structure, or they were peddling third- and fourth-party technologies bundled together. It was like trying to work with a building contractor who couldn't tell you how many doors or windows you would get in your house, or how much the roof would cost. Only a few could meet some of our principles. Only one could really meet them all."

Selecting an Open, Flexible Tokenization and Cloud Data Vaulting Platform

The selection of the TokenEx Data Security Platform to secure all three of Orvis' channels and remove all PCI and personally identifiable information (PII) from the business systems resulted from the TokenEx team's ability to clearly articulate the five principles and how they would be put into action.

1. The ability to use the same cloud tokenization architecture to secure the e-commerce web site, the contact center, and the retail point-of-sale card readers in stores and in the field.
2. A clear and predictable pricing structure for tokenization and data vaulting, where there is a single charge for tokenizing and vaulting each PAN and PII datum, with no additional charges for accessing the vaulted data for transactions.
3. Integrating the processes for encrypting and tokenizing sensitive data required no changes to the existing business processes and was transparent to associates and customers alike.
4. All data types—not just payment card data—could be tokenized and securely vaulted using the same processes.
5. The architecture of the end result was clearly diagrammed and documented before sales contracts were signed, providing an assurance that TokenEx could deliver all the necessary P2PE device interfaces, Web APIs, encryption key management, and secure data storage for all the geographically dispersed retail channels and operations.

In addition to meeting all the primary qualifications, TokenEx could also offer:

- The ability to interface with any payment processor or gateway to ensure that Orvis has the freedom to add or change financial partnerships to keep growing globally.
- A guarantee that should business requirements dictate, all tokens and sensitive customer data will be returned to Orvis on demand—part of TokenEx business philosophy that a client's data is always the client's data and TokenEx is the custodian only for as long as the client needs.
- As data privacy regulations—such as GDPR—become effective and evolve, TokenEx will ensure that personal data held in its vaults is treated appropriately, which will be critical for organizations doing business in the Eurozone.

Implementing the TokenEx Tokenization and Data Privacy Platform Worldwide in Five Months

The Orvis Company is a highly distributed organization of retail stores in the US and UK, and adventure travel experiences worldwide. At the center are the two regional e-commerce web sites for the US and UK as well as contact centers for call-in orders and email processing. Integrating the TokenEx Data Security Platform was a multi-step process that was carefully mapped out before deployment to ensure that all touch points where payment and personal data entered the business systems was captured, encrypted, tokenized, and vaulted. Only the tokens representing the sensitive data are returned to the Orvis databases and order processing systems.

In keeping with the first principle articulated by CISO Martin, every channel was integrated using the core technologies built into the TokenEx Data Security Platform: encryption and key management, tokenization, and cloud data vaulting. The entire integration process took about five months, from deployment of encryption keys, testing of e-commerce web APIs, and tokenization and vaulting of existing PANs.

The Orvis retail stores are equipped with Point to Point Encrypted (P2PE) Payment Card Readers at the point of sale (POS) stations. Each of the P2PE readers are programmed with a TokenEx Public Encryption Key so that as cards are swiped, dipped, or tapped the PANs are instantly encrypted and can only be decrypted by TokenEx using the paired private key. Associates in the field for adventure travel use mobile P2PE readers and PANs are encrypted and saved in the local device for nightly uploading, batch tokenization and payment processing.

In the contact centers, agents taking customer orders over the phone use physical and virtual window's machines that are directly linked with the P2PE card readers. Similar to the retail store POS, PANs are instantly encrypted in the card reader and transmitted to TokenEx for tokenization and vaulting. The actual PAN is never received by the contact center computer, keeping those devices out of the scope of PCI compliance.

At the e-commerce Orvis web sites where thousands of customer orders are received every day, payment card data is intercepted using the TokenEx Browser-based Encryption API. Once again, the PANs are never received by the Orvis web servers, but routed directly to TokenEx Cloud Vaults to be tokenized and stored. The paired token is sent back to the Orvis web server and back-office systems for payment processing when the order is physically shipped. As orders are shipped, Orvis transmits the tokens in batch mode to TokenEx where the batch file is translated back to encrypted PANs and sent to the financial partner for payment processing.

Open Integration Platform Key to Securing Third-Party Service Providers

With operations in North America and the United Kingdom, plus travel associates worldwide, other third-party services and payment processors were also part of the integration plan. TokenEx Open Integration Platform acts as a central hub with many services, such as credit approval, fraud detection, and gift card providers, as well as financial institutions. In the case of Orvis, TokenEx integrates with Chase in the US and FirstBankcard in the UK, in addition to GiveX gift cards. It's the flexibility of TokenEx that provides clients like Orvis with the freedom of choice to work with the partners they choose, and are not limited to one or two service providers.

TokenEx Provides Bespoke Service

Martin reflects back on the project and TokenEx's role: "TokenEx is very efficient but they're also willing to be bespoke in the manner you need to be bespoke. For example, we wanted a specific custom token scheme. They provided us with a proposal to do the work, and it was done efficiently within the time when it was necessary—and the cost was very affordable. Really, the TokenEx platform is designed to plug it in and do everything you need it to do. Just that small deviation made it more efficient for us."

"Over the five months of integration we didn't even need to have any people dedicated to the tokenization project, other projects were ongoing at the same time. It really went smoothly. At the end we achieved a rather remarkable 90% reduction in PCI scope. All the payment card data is safely removed from our internal systems and stored with TokenEx. We never touch any payment data in our contact centers, retail stores, web site or in the field. And that's a big relief."

Reduce Risk of Data Theft and the Cost of PCI Compliance with TokenEx

The TokenEx Cloud Data Security Platform secures all types of sensitive data, keeping business systems free of data theft risk while enabling essential processes to operate unchanged. From property management systems, to contact centers, retail POS, and ecommerce web-stores, TokenEx stands ready to protect sensitive data. Remember, No Data, No Theft.

Contact TokenEx at **sales@tokenex.com** to get a personal review of your data security risks and how cloud tokenization can protect your customer data and your brand.