TOKENEX

h2O® WIRELESS

Card Easy™
Keypad payment by phone

Locus H2O Wireless removes PCI risk from omni-channel contact center

A Four Week Integration with TokenEx Cloud Tokenization and Syntec's CardEasy Keypad Payment by Phone

The Contact Center as Payment Hub and Security Risk

For many organizations, the contact center is becoming the nexus of omni-channel commerce. Incorporating Interactive Voice Recognition (IVR) systems, live agents, chat bots, and web portals, what was once a problem-solving support center is now the focal point of payments that flow from customers through telephony lines. But with that shift comes the great responsibility of securing the payment and personal information that is collected, stored, and processed by agents and automated devices.

Contact centers with human agents that accept payment card information must conform to the highest levels of the PCI Data Security Standard (DSS)—an expensive, time-consuming, and ongoing process. However, by removing all payment card information from the conversation between customers and live or automated agents, re-routing the sensitive data out of internal business systems, and storing only tokenized data, PCI compliance can be greatly reduced and the call center secured from data attacks. That was, in fact, the goal of Carlos Moreno, Payment and Fraud Analyst, at Locus Telecommunications, as his team tackled the security of their omni-channel contact center for the H2O Wireless brand.

H2O Wireless provides their customers with pre-paid cellular services, both through direct and indirect sales. Customers choose a plan that meets their data, text, and voice needs and pay a set monthly fee, with no contract or hidden fees. Customers can choose to recharge their phones each month by calling into the contact centers or going through a web portal and providing their payment information. Tech-savvy customers can use the web portal or IVR, or new customers can interface with an agent for personal help. Loyal customers can also choose to enroll in a recurring billing plan, so each month their phone is automatically recharged, usually with a discount and other benefits. In all these channels, customer payment and personal information is captured by human or software systems, stored, and reused as needed to keep customers online and satisfied with service levels.

However, with a growing and successful business, the amount of sensitive data being exposed to human agents and managed within H2O Wireless' systems was becoming enormous. Processing over 350,000 transactions a month, 3.6 million transactions every year, and increasing, the business was heading for a data security storm. Complicating matters, Locus had built sophisticated home-grown CRM and back-office financial systems—some of which are patented—specifically tailored to meet the organization's business needs. These specialized systems handled and processed all the payment and customer account data for multiple business units. However, since human agents were exposed to the incoming sensitive data, keeping these on-premise systems and the contact center in compliance with PCI DSS was a massive effort. New Euro-zone data privacy regulations, such as GDPR, that are on the horizon will require even more security over personal information for international organizations.

To Carlos Moreno, keeping that all that sensitive data from ever entering H2O Wireless systems–without altering their existing IT applications—became a critical project for the financial security team. "Even though we were using very strong encryption models to protect the payment and personal information, it was still passing through and being managed by our systems, “says Moreno. “Critically, our human agents in the contact center were being exposed to payment account numbers over the phone, creating a tricky PCI compliance problem. We needed to get rid of that step as well.”

Carlos Moreno explains, “There were two important components to the project. Number one was making sure that we are able to obtain and maintain PCI compliance by reducing the scope of payment acceptance as much as we could. And number two, perhaps more importantly, was to make sure that we are actually securing the personal account information of our customers so that in the event of a breach or a cyber-attack, that information is stored outside of our environment where it cannot be accessed.”

Searching for an Open and Flexible Security Platform

The first step of reducing the scope of PCI compliance entailed choosing a security platform that could not only provide the necessary tokenization of payment data before it entered H2O Wireless systems, but vault it off-premise. The most critical requirement however, was to find a tokenization vendor that could integrate with the existing H2O Wireless systems and business processes and require very minimal changes to them. “We vetted several tokenization vendors including our existing payment processor” says Moreno. “It was my responsibility to find and recommend a security partner that could integrate with our existing systems and service all our business units. We could not do this project if we had to spend years modifying or replacing our software with off-the-shelf CRM and back-office applications. We also couldn’t afford to disrupt existing business processes in the contact center or back-office. So integration flexibility was key. Fortunately, we found the ideal partner in TokenEx.”

The TokenEx Cloud Security Platform is a flexible and open solution to intercepting payment data, turning sensitive data into tokens (the tokenization process), and storing the real data, personal or payment, in secure cloud data vaults. Tokens are returned to the client systems to be used for payment processing and account management. After a successful tokenization project, sensitive data is never accepted, stored, or transmitted by the client’s internal business systems. In this way, business processes continue functioning as usual using tokens, so that should a breach occur, no sensitive data is exposed. As a result, the scope of PCI compliance is greatly reduced to a few PCI DSS Self-Assessment Questionnaire (SAQ) points, at a much lower cost and overhead.

Integration and Portability Key to Rapid and Cost-Effective Implementation

The integration of the TokenEx platform required only two weeks of planning, coding, and testing. Moreno was duly impressed with the initial integration of the tokenization process: “I have extensive experience working with all sorts of providers and vendors within the payment card ecosystem. I can speak with 100 percent certainty that TokenEx has been, since day one, one of the most responsive and most engaging vendors that I have ever had the pleasure of working with. From the sales team that gave us accurate and reasonable price quotes to working with their technical team. Within just a couple of days of speaking with them we had APIs to begin working with as well as integration documentation—before we even executed a service agreement. That gave us a lot of confidence that TokenEx was a true partner in this endeavor.”

Other key reasons Moreno chose to work with TokenEx was the integration and portability capabilities inherent in the platform. TokenEx’s open security platform adapts readily to a wide-variety of ERP and e-commerce software systems, even H2O Wireless’ custom and proprietary software. “TokenEx provided the flexibility which gave us the convenience of not having to change any of our internal processes or modify our IT systems. TokenEx was able to customize their solutions for us. That flexibility alone saved us hundreds of thousands of dollars by avoiding buying and implementing new software, not to mention the time that it would have taken to implement. Open integration is key."

In another example of openness, the tokens created by TokenEx are portable among the many payment gateways and financial processors, so they can be used transparently among a variety of vendors. "It's an additional proof of TokenEx openness that they give us the flexibility to have tokens that are portable and available in the event we ever wanted to switch payment processors or if we wanted to have more than one single-processor relationship," says Moreno. In addition, TokenEx's openness policy guarantees that a client's data is always the client's data and will be returned upon request with the paired tokens. Many payment processors that provide tokenization services use proprietary format tokens that will not be provided to the client should they decide to change vendors and would not work with other providers even if they were available.

With the initial integration complete, all the existing payment and personal account data that had been stored in H2O Wireless' systems was replaced with tokens, and the customer data safely stored in TokenEx Cloud Data Vaults. When a customer payment needs to be processed, the H2O Wireless systems passes the matching token to TokenEx, where it is swapped with the actual payment data and sent to the payment gateway for authorization and processing. The actual payment account numbers (PAN) are never stored or transmitted by H2O Wireless systems.

Diverting Incoming Payment Card Data to the Cloud with Syntec CardEasy

However, to reduce PCI Compliance to the absolute minimum, there still remained the initial receipt of PANs through the contact center via a live agent or the IVR system. The existing system let customers enter their payment information through DTMF (Dual Tone Multiple Frequency or Touch-Tone signaling) keypads on landline or mobile phones, but the human element was still on the line and could conceivably intercept the PAN. Likewise, with the IVR, the PAN was still being received and decoded from the DTMF signals and recorded in the contact center system. This process keeps the contact center in scope for PCI compliance and is difficult to monitor.

While initially Moreno assumed TokenEx could intercept the incoming DTMF signals and tokenize them directly, that was not possible given the telephony interface. There needed to be a method of digitizing the tones first. Even though TokenEx could not do that out of the box, they had an established partner that could —UK-based Syntec and its patented CardEasy keypad payment by phone DTMF system. CardEasy can be deployed as a cloud service, integrating with the TokenEx cloud platform, to ensure that payment card numbers never enter the contact center environment.

Syntec's CardEasy system was also quick to implement. CardEasy interfaces with any telephone call center solution and back-office system out of the box. It intercepts the DTMF tones representing the customer-entered PANs, decodes them and, in the H2O Wireless implementation, sends the PANs directly to TokenEx to be tokenized and stored. Agents and the IVR system never hear, see, or receive the digits or tones for the complete PANs, so they are not available for capture in call center systems or call recordings, thereby keeping the contact center out of scope for PCI compliance.

"We chose Syntec because they had the solution that we needed to de-scope our live contact center agent and IVR environment. Syntec was the only vendor that provided the flexibility to integrate with our home-grown systems because their system can be cloud based, with no requirement to change any of our existing IT. The same flexibility offered by TokenEx was offered by Syntec," says Moreno. During the two weeks it took to implement, integrate with TokenEx, and test, Syntec's team of developers was always available to ensure that any interface could be made compatible with H2O Wireless' systems.

"So not only did TokenEx make integration extremely easy with rapid responses to technical issues, and their ability to quickly make changes to their APIs, they can also provide a seamless end-to end service in partnership with Syntec to fully de-scope the contact center from PCI DSS and remove any security concerns. This is one reason why the project became a reality—because of the TokenEx team's ability to look beyond the services that they have and provide us with additional tools."

Achieving a PCI Compliant Contact Center in Four Weeks

Carlos Moreno summarizes the success of the project with two quantifiable and significant savings. "One of the biggest savings is something that we were able to quantify from the very beginning—that we could keep our homegrown systems as they are. We didn't have to spend any effort or funding to integrate something new or change our payment strategy. We're talking about potential savings over nearly half a million dollars if we had to purchase just a new CRM system—not even counting the manpower and time it would take. Looking at savings for PCI compliance, if we had to create our own PCI Island with separate servers and databases to isolate the contact center, the hardware costs alone would be onerous. Being able to work with TokenEx and Syntec to become PCI compliant with no changes to our operations and IT infrastructure is a huge benefit. Doing so in four weeks is really a great way to measure success."

Tokenization and Cloud Data Vaulting Saves Big on PCI Compliance Costs

While PCI compliance is a necessity for organizations taking omni-channel payments, the cost of compliance coupled with the risk of data theft are growing business pain points. Whether your business data is payment, personally identifiable, healthcare (PHI), or document/image-based, the risk of exposing it to data thieves can be eliminated through a combination of encryption, tokenization, cloud data vaulting, and key management. The TokenEx Cloud Security Platform employs all four of these techniques to remove sensitive data from IT systems without disrupting existing business processes. The open integration capabilities of the TokenEx platform provide proven methods of working with other technology providers to securely accept payments and move sensitive data among your choice of payment partners. With TokenEx acting as custodian, your data is always your data, with a no-caveat return policy should your business needs change. The TokenEx team is at your service 24x7x365 to ensure that your sensitive customer and payment data is available and secure. Remember: No Data, No Theft.

Need help with securing sensitive data of any type for your organization? Contact TokenEx at **sales@tokenex.com** or call US (877) 316-4544

For more information on the Syntec CardEasy, send an email request to **sales@cardeasy.com** or call (US) (303) 500-0492 or (UK) +44 (0)20 7741 8000