Locus

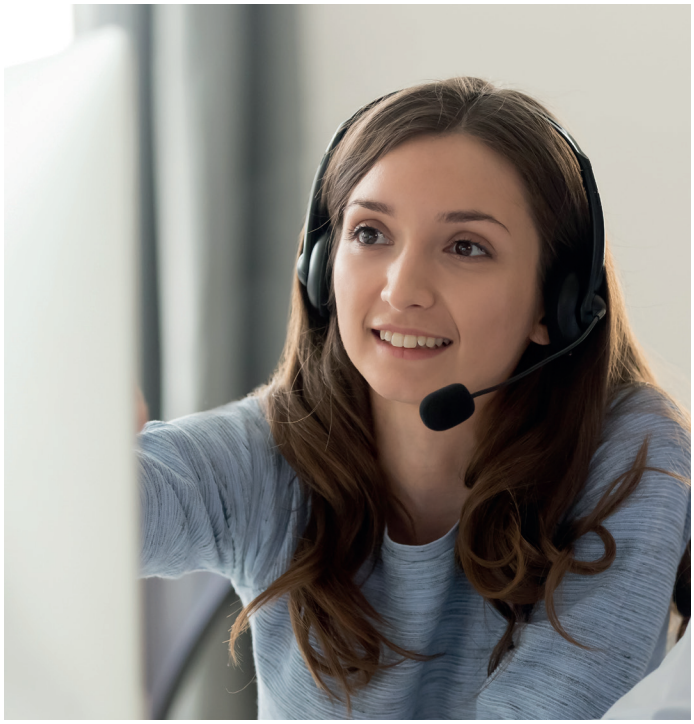
an NTT DATA Company

H2O Wireless provides its 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. Tech-savvy customers can use the web portal or IVR, or new customers can get personal help from an agent. In all these channels customer payment and personal information is captured by human or software systems, stored and reused as needed. The organisation processes over 350,000 transactions a month, 3.6 million transactions every year, and this number is increasing.

A four week integration with TokenEx cloud tokenization and Syntec's CardEasy keypad payment by phone in the US

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 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 tokenised data, PCI compliance can be greatly reduced and the call center secured from data attacks.



The challenge facing H2O Wireless

H2O Wireless provides its 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. Tech-savvy customers can use the web portal or IVR, or new customers can get personal help from an agent. In all these channels customer payment and personal information is captured by human or software systems, stored and reused as needed. The organization processes over 350,000 transactions a month, 3.6 million transactions every year, and this number is increasing.

Locus has bespoke CRM and back-office financial systems tailored to meet its business needs. These specialised systems process all payment and customer account data for multiple business units including H2O. 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 require even more security over personal information for international organizations.

H2O's key objective was to keep the sensitive data from entering its systems, but without having to altering the existing IT applications.

> "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. 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**
> Payment and Fraud Analyst, Locus Telecommunications

> "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."
>
> **Carlos Moreno**
> Payment and Fraud Analyst, Locus Telecommunications

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. The TokenEx Cloud Security Platform fitted the bill.

The TokenEx Cloud Security Platform is a flexible and open solution which intercepts payment data, turns sensitive data into tokens (the tokenization process), and stores the real data, personal or payment, in secure cloud data vaults. Tokens are returned to the client's systems to be used for payment processing and account management. This means that 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 and, 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 points, at a much lower cost and overhead.

Diverting incoming payment card data to the cloud with Syntec CardEasy

However, to reduce PCI compliance requirements 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 signalling) keypads on landline or mobile phones, but the human agent 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.

TokenEx could not intercept the incoming DTMF signals and tokenise them directly – they had to be digitised first using Syntec's 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 tokenised 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."
>
> **Carlos Moreno**
> Payment and Fraud Analyst, Locus Telecommunications

Achieving a PCI compliant contact center in four weeks

Carlos Moreno summarises 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."
>
> **Carlos Moreno**
> Payment and Fraud Analyst, Locus Telecommunications

"We chose Syntec because they had the solution that we needed to de-scope our live contact centre 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."

For further information, or to read other case studies, please visit:

www.cardeasy.com