CCW Vegas 2019 - Semafone

Semafone

Gary Barnett, CEO, Semafone, sat down with CRMXchange to talk about how the company provides simple, fast, cost-effective PCI DSS compliance and data security for contact center environments.

Gary, would you like to tell us how you got involved with Semafone?

It started when I did some work for Semafone's board of directors late last year. I've been in the contact center business for a long time, but one of my greatest passions is bringing the great add-on capabilities to the market. Data security is one of those great new disciplines to which every company must adhere. I simply fell in love with what the company is now accomplishing and how well it fits the direction of the marketplace. It's also unusual to have a company that started out internationally and is expanding and moving to the U S. After I began working with Semafone in October, 2018, I wound up joining the company as the chief executive officer this past February. It's been a fantastic experience to work with the team.

Can you elaborate on what the solution is designed to accomplish and why businesses should be interested?

It's quite easy to explain. Most consumers know what it's like to pay through a contact center. We can call an airline and when they respond that they can book a reservation, the next question is 'what is your credit card number?' The issue with that process is that it's not compliant with PCI regulations. It leaves a person's credit card number exposed. The agent or someone sitting next to them in the contact center hears it and could easily copy the numbers. Companies also store multitudes of credit card numbers which can and have been breached. We've all read articles in the *Wall Street Journal* about millions of credit card numbers escaping to the open world. What Semafone does is enable contact centers -whether on premise or cloud-based – to reduce risk and take secure credit card payments on the phone and through other channels as well. One way to protect sensitive information is to ensure none of it is stored. You can't steal what you don't store. Even though no information is kept as available records, the consumers' payment is processed.

Here's where our difference comes in. The agent confirms they can take an order, but instead of asking the customer to read credit card numbers, they instruct them to enter it on their phone's touch tone pad. While the voice interaction can continue as the customer enters the information, the agent never hears the DTMF tones and has no way of finding out what credit card number the customer is using and the sensitive information is never stored. Our solution enables the number to be processed to the payment provider, at which point the agent can verbally confirm that it went through. As such, an agent can thus provide exceptional customer service with no immediate or long-term security risk.

While we've positioned ourselves as an industry leader in secure voice transactions, we've also moved into the digital world. When a business asks a customer in a chat conversation to make a payment to place an order, it's understandable that the customer would be concerned about entering sensitive information. Our solution enables the agent to reassure customers that they will be put into a secure transaction where no one will be able to see what credit card number is being entered. Just as in our solution for protecting voice payments, the agent will be aware of the customer's progress and if the payment has been accepted and nothing more. Customers have the same level of security in SMS or email or even social media.

What does the consumer who is told they are in a secure payment environment see during the transaction?

We employ a very clever user interface which we put a great deal of thought into creating. First and foremost, it must be secure. Second, we want to make it an enjoyable experience with a certain 'wow' factor involved. The agent remains with the customer but not in the same chat window while the information is being entered. The customer sees a picture of a credit card and can fill their numbers in on the surface. When it's time to type in the CVC, the credit card visual rotates to where they enter it. Simultaneously, the agent on the other end can verify that the customer has successfully entered the credit card number. None of the credit card information is ever visible in the agent's chat window.

Of course, our customers still get audited and are required to get their PCI DSS compliance certified. However, it's much easier for them to receive because we've separated all secure information. Therefore, when the QSA examines the auditing, they're not concerned with agent accountability or possible breaches. Our customers like it because we centralize the security as opposed to it having to touch 20 different systems and our clients don't miss a second of the recording – as it's the same in chat transactions.

Does using your solution make information less hackable and more secure than if the company was taking the information?

In terms of securing credit card data, the saying we like to use is "They can't hack what you don't hold!" Semafone's Cardprotect solution prevents cardholder data from ever entering the business infrastructure, so organizations do not have to worry about hackers accessing it—as there's nothing for hackers to get ahold of in the first place.

Once a transaction has been done, it's gone?

We ensure there is no long-term storage, and in the fleeting moment when a number exists as the system processes payment, we are absolutely protecting that transaction. Once it's over, our customers don't need to think about it again.

What kind of companies are best served using your solution?

Excellent question. We see conservative businesses such as insurance companies that take payments on the phone or through digital transactions that want to make sure they are fully compliant and not just PCI DSS compliant. We work with other companies such as retailers which have a very high volume of payments on the phone or through the contact center. We also work with healthcare organizations which need to do more than simply protect credit card information but also secure member IDs or social security numbers. There's one additional interesting category; companies which have been hacked and having learned their lesson, want to ensure that it never happens to them again.

When I'm shopping online, even if it's a site I use frequently, I always decline when asked if I'd like them to store my credit card information. Do you see business ending that practice to limit their liability?

While some people see that as a convenience, enabling a company to keep your credit card on file would only be acceptable under very limited circumstances. We would certainly highly recommend that those companies use a process called tokenization. In that scenario, the card information goes to the payment provider and the payment provider comes back with a token. If someone were to steal them, the tokens would almost always be useless. No one should even consider allowing a business to store their credit card numbers in the clear. The next worst thing is the storage of credit card numbers that are encrypted. Our advice is don't store at all or at the very least ensure that information is tokenized by the payment providers.

Is there anything more that you think our audience should know about Semafone?

The thing that amazes me is that in the US market, one of our most pressing concerns is how do we help educate the industry? Many people in the contact center space claim to understand it, but in most cases, they don't. This translates into numerous companies that believe they're protected when they are extremely vulnerable, or not protected at the level they need to be. Helping to build this crucial knowledge makes it a high value market with a great upside. One of our key goals is to get executives to understand what's real, what's not, what's important and what's not. We provide a valuable solution and the more people know about the need for it, the more opportunity we have for growth.