ceocfointerviews.com

Issue: May 5, 2014
The Most Powerful Name in Corporate News

EMV Chip Issuance Cards for Secure Transactions

Joan Ziegler - *CEO*

FiTeq Financial Technologies takes payment card solutions to the next level. FiTeq EMV Cards are the only proven and available solution for magnetic stripe issuers to bridge to EMV chip issuance with immediate benefits, regardless of the point of sale, and protects the investment of current EMV chip issuers globally when their cards are used in non-Chip environments. FiTeq EMV Cards and FiTeq Authenticator Software create exceptional value to banks, enabling a solid ROI from fraud reduction and unprecedented innovation in card services. To ensure safe, secure and convenient transactions anytime, anywhere, FiTeq's core technologies include the FiTeq Energizer Stripe (changes magnetic stripe data dynamically) and the FiTeq Transaction Specific Code (ensures cardholder data cannot be reused fraudulently and can provide additional value added services). Incorporated in 2008, FiTeq is privately held and has licensed the patented technology in each of the over 100 million US contactless cards already in use. FiTeq Financial Technologies is based in Tiburon, California. FiTeq Financial Technologies – Powering Innovation in Payments.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

CEOCFO: ***Ms. Ziegler, your site shows FiTeq is powering innovation and payments. How so?***
Ms. Ziegler: We are a company that is really putting a stop to the losses and the operational expense of data breaches. I am sure you heard of the Target data breach or Neiman Marcus. Everyone is focusing on the breach being the problem. What FiTeq does is instead of focusing just on the breaches, we have engineered a way to change the magnetic stripe data and your three digit code that you plug into an ecommerce site. When those nasty, pesky breaches happen, the data cannot be reused by the fraudsters, so it cannot be used for a second transaction on a counterfeit card.

CEOCFO: ***Would you tell us how the technology works?***
Ms. Ziegler: The technology is that new kind of card you might have heard about in the news, an EMV card. There is a processor chip on the card and to get the full advantage of that EMV chip on the card, all of the merchants need to change their back end infrastructure and they need new terminals because it is not swiping like with the magnetic stripe. We take the cryptography from that card, and using the cryptography in that EMV chip, we populate a cryptogram inside the mag stripe but it is readable by the existing terminals that are out there today, the regular mag stripe terminals. If you are doing an e-commerce transaction, we give you dynamic data when they prompt you for those three digits.

CEOCFO: ***Are people using this today or is it still in the development stage?***
Ms. Ziegler: We are just at the point of bringing the technology out in a major way. We have been testing under the radar with a number of banks both here in the US and abroad. What is really key to satisfy banks who are very discriminating in the technologies that they adopt is they have a pretty exhaustive certification process for new products. We have been qualifying the technology and running both internal tests and third party lab tests and we are right at that point where we are ready to launch, so you called at the right time.

CEOCFO: ***Do people believe that it will work?***
Ms. Ziegler: It is something novel. Mag stripe has been around since the 50s, so they have not gone charging into the 21 century too quickly. I think what is key is there are a number of different companies that have tried new technologies for payments. Generally, the vexing part of the new technology is that if it is a new device for the consumer, the merchants also have to adopt. What is really the key to success to MasterCard, Visa etc. is what has really made those payment methods successful, which is whether you are in Shanghai, Paris or LA or in Florida, where ever you go, you can whip out

your card and the merchants can accept it. Likewise, with telephone orders or internet orders, you have to flip over the card and grab those three digits and put them in the E-commerce form. If people do not recall anything else about what our technology does, the one thing they really appreciate and understand is that this is a solution that merchants have to make no change whatsoever.

CEOCFO: *How do you generate a new three digit code?*
Ms. Ziegler: We rely on that EMV chip and the EMV standard for Europay, MasterCard and Visa. What is really key about that is if you fit all of the rules, it helps with mass adoption. The cryptography in their approved EMV chips is what we rely on. We have our own algorithm but we make sure we run our algorithm on an EMV compliant chip and we make sure that we follow all of their rules. That certainly greases the skids to help us be successfully established in the marketplace.

CEOCFO: *What is the competitive landscape today?*
Ms. Ziegler: There are a ton of innovative approaches now to payments. We are one layer of this layered approach to technology. You can do EMV chips and they are really great, although to get the full benefit of just the EMV chip, you have to get all of the merchants to adopt at the same time. EMV is out there and we are an EMV chip solution. What differentiates us is that we have impact day one because the security works on all terminals. There is also Point-to-Point encryption, End-to-End encryption and I think every opportunity that is there to make more secure a cardholder's data is a good thing. There is encryption in that pipe that sends the transaction back to the issuing bank, but as you have seen with Target, Neiman Marcus or Sony, they can be compromised. It is a number of solutions that will make the payment card industry more secure, so layering up and introducing greater innovation I think is the path forward for payments. With the FiTeq solution, the bad guys cannot slip in there, sniff the cardholder's data and find a way to reuse it on a counterfeit card.

"We are a company that is really putting a stop to the losses and the operational expense of data breaches. I am sure you heard of the Target data breach or Neiman Marcus. Everyone is focusing on the breach being the problem. What FiTeq does is instead of focusing just on the breaches, we have engineered a way to change the magnetic stripe data and your three digit code that you plug into an ecommerce site. When those nasty, pesky breaches happen, the data cannot be reused by the fraudsters, so it cannot be used for a second transaction on a counterfeit card." - Joan Ziegler

CEOCFO: *What do you see as the barriers to gaining acceptance?*
Ms. Ziegler: We as a company have made a conscious decision to be very quiet, to work under the radar and really focus on two things. One thing is consumers; listen to consumers. What do they want? Why are breaches bothersome to them? What can they do to be protected all of the time? Then, there are a number of marketing opportunities we have with this technology as well. Instead of getting ahead of ourselves and building the Rolls Royce, we have really listened to what consumers' want and consumers are very concerned about their credit and debit card safety. Research we ran with Penn Schoen Berland told us that they are more worried about data breaches and identity theft than even food safety or terrorism. Initially, I looked at the results of that research and I did not know how that could possibly be. For example, if there is a problem with the chicken you purchase at your grocer, you get the news alert right away and you know not to buy that brand. Similarly, with regard to terrorism, you need only to go fly anywhere in the US and you realize how things have really dialed up and changed security-wise. Conversely, however, when it comes to payment cards, the breaches seemingly go on and on and there is probably nothing more vexing to a consumer than to receive that call or email that says they have to send you a new card in the mail because your card has been breached. Consumers have become pretty savvy and said "Gee, who is looking out for me?" We really tried to understand what the consumer wants. If we can create a payment card technology that consumers really want, then the bank that is the first mover gets a huge advantage and we saw extraordinary gains for the brands of the banks that adopt this technology from the research we conducted. We have surely shared that information with the banks. There is an absolute bump in trust of the banks and their brand when customers of their bank or other banks were asked if "such and such" bank adopted this technology, would they be more likely to trust them and more likely to move their account to that bank. We think if you really pay close attention to the consumers, stay consumer centric, we bring even greater value to the bank because it is not just fighting fraud, it is not just fighting all the operational expense of reaching out to consumers, saying we have to replace your card. It is building a relationship and it is about building trust between that bank's brand and the cardholder. The savvy banks that do like to be first movers with new technologies are very excited about this technology. We are just launching now. All of the consumer testing and the bank's testing has been done under the radar. There is not much noise. We make certain

we are satisfying what those consumers want. As always, with any product, if you deliver value, the brand that is delivering it becomes much more meaningful to a consumer.

CEOCFO: ***What is the strategy for the next six months to a year?***
Ms. Ziegler: The next steps for us are here in the US where there is extraordinary awareness. Unfortunately for Target, they have made it very clear to consumers what the issue is. For us, concentrating on the first movers here in the US market is priority one and we are just in the process of making that happen right now. We are presently finishing the certification with the major networks. The next step for us is launching in other places in the world that are looking to close some of those security gaps that exist. I think for us, there are two international markets that are very appealing and have this need. Though these markets have already gone to EMV chips cards, the one area that EMV does NOT address is for "card not present" sales when you do E-commerce or when you are giving that three digit code over the phone. This is where we are putting a dynamic number in a flexible display actually positioned on the card, so you do not have those same static three digits every time. (There are four digits if an American Express card. So the two markets we have really targeted, outside the US, start with Europe as we have some very keen interest from some of those issuing banks because that will really help them control fraud from E-commerce and phone orders. The other market that is also an EMV territory is in Brazil and the rest of Latin America. They have very good adoption and they have changed out their readers at retail. Some of the bad guys in Brazil realized that maybe Brazil has EMV, but if they crossover into another territory in South America, they do not have those EMV chip readers, so they can go ahead and swipe the card and it is called "Fraud Abroad". That is really our strategy, US first and then Europe and Brazil simultaneously. That keeps my business partner, our team and myself really busy.

CEOCFO: ***How does this work over the phone and E-commerce?***
Ms. Ziegler: Today when you are on the phone with your airline, even if you have a frequent flyer number, they are going to say "Can you tell us the three digits on the back of your card?" You do not have to report the card number, they store that, but they do not store those three digits. Because those three digits on the back of your card are static, if the bad guys are smart enough to hack into Target and Neiman Marcus, you can bet they are smart enough to capture those static three digits on the back. So, instead of having it be static, we have a display on the card that has three digits and you press a button that says give me a new set of numbers every time you are on the phone or online. It says, "Press Here" for new card security code - right on the card. These are powered cards that have a little battery inside. Once those three digits have been used, those three digits cannot be reused again.

CEOCFO: ***Do you have the team in place and do you have the funding to reach out to the various potential early customers?***
Ms. Ziegler: I think that we have been very fortunate as a company. We have a handful of investors and they are long term investors. As you know, with Silicon Valley start-ups, there is an expectation that things are going to move really quickly. One thing we know about the banking business and payment cards is it is going to be a slower adoption level than what would be a typical Silicon Valley deal. Knowing the market, we were definitely fortunate to identify long term investors that really appreciate what our long term vision is and saw us through the development phase and all of this final testing that we are doing right now. When we get into broader distribution and the next phase that would be more like Mezzanine Financing - which is definitely a high class problem to have! - We are looking forward to the challenges of meeting demand in the marketplace.

CEOCFO: ***Put it together for our readers. Why pay attention today to FiTeq?***
Ms. Ziegler: I think what Target has done is really make this top of mind and Target's CFO was on Capitol Hill yesterday. There are different financial services, committees, and judiciaries, both in the House and in the Senate. I think there is a good bit of discussion in the press and out there in general demand from the public, how these types of problems should be resolved. Should it be government mandate? Should it be MasterCard and Visa alone setting the standards? Should it be layers of innovation? I think just free market, the US way of building the better mousetrap, inviting innovation in payments and having layers of security is definitely the way to go forward. This is something that we have been engineering for some time and it has really been the highlights around the Target breach that clarify for the consumers, for the banks and for the government how critically important this is. I personally had fraud at my bank and I love my bank but once you have fraud on your card, it can lead to identity theft. One in three compromised cards experience identity theft. I therefore do not think we could be timelier in our launch. I truly believe that FiTeq is just the right antidote for the problems facing the payment card industry now.

FiTeq

566 Minnesota St
San Francisco, California
415.435.4500
www.fiteq.com