What's new in FinTech security?

Date: *Tue, 10/17/2017 - 13:36* Source:

The world was still reeling from the breadth and depth of the Equifax hack when I attended a session on Security Innovation in the FinTech Sector at last month's NetEvents Global Press & Analyst Summit in San Jose, California

Ondot's CEO, Bharghavan Vaduvur

Image credited to NetEvents

The session was chaired by Global Data's Senior Analyst on Enterprise Security, Eric Parizo; and the three panellists were: Ondot's CEO, Bharghavan Vaduvur; McKinsey & Company Partner, Robert Schiff; and Technology Credit Union's SVP of Information Security, Ratnendu Mukherjee. Also interviewed was Ron Green, MasterCard's executive VP and CSO.

"First topic, we're going to talk little a bit about the Equifax breach… that, based on media reports so far, has involved a breach of up to 143 million consumer credit records here in the US and a few hundred thousand people internationally", Eric Parizo was setting the scene for a discussion that could not have been more timely and, as Ron green put it: "The financial industry is a big target because of the nature of what it does, you know attackers go to where the money is and so that's why the financial industry is a high-value target".
News was still coming out about the breach – the number of victims would rise to 145.5million – and, as Parizo pointed out, that meant the majority of American adults were affected. "So", he asked the panel, "is there anything about this breach incident that is new or different versus other incidents?"

The basic answer was "no", this was a pretty typical breach in technological terms. What made it outstanding was its scale and its extent of influence. As Ratnendu Mukherjee explained: "It was pretty much known early on that it's not 'if', it's a matter of 'when' – when multiple organisations will get targeted. So in terms of the uniqueness of the Equifax breach, it's not anything new." The greater long-term damage, Parizo suggested, was the damage to public trust.

A hacked credit card is bad news for everyone concerned, but the card owner has at least made a conscious choice to apply for that card and is aware of the potential risk. But much of the data held by a credit agency like Equifax has been collected less directly – people might not even be aware they are on the Equifax database – and it includes a wider range of data, including names, addresses, phone numbers, Social Security numbers and data that has lasting value for identity theft. You can change your credit card on the spot, but you are not going to change long term data in a hurry.

Bharghavan Vaduvur from Ondot pointed out that breaching identity is a lot more widespread than breaching a card and the solution is a lot more complex. The whole purpose of the Equifax bureau is to capture and consolidate all the information about the individual, so that merchants can KYC (Know Your Customer) and identify individuals' identity. If the identity is breached, solving the problem becomes far more challenging. Trust was further compromised by the way that Equifax had handled the news, according to Parizo: “Equifax has been widely criticised for not responding effectively in the early days following the breach. It's difficult for consumers to find out if they actually were affected. The website [created so people could check if they were affected] didn't work well, their call centres couldn't handle the load, they had a lot of problems.” It was also claimed that they knew about the breach long before it was made public.

Reduced trust in FinTech would probably first hit online sales, as Robert Schiff explained: “In general, there is more confidence in making a transaction at a retail point of sale, where you see someone and swipe your own card, than doing it online.” He also suggested that online people would still trust the giants like Amazon, but it would hit smaller merchants who would bear the burden of rebuilding consumer confidence.

Parizo moved the discussion forwards by asking about ultimate responsibility. As Green had put it: “One of the largest concerns is that, while we have to partner with a lot of service providers in order to deliver the services to our consumers, the challenge is how do we make the service providers be accountable and maintain the confidential information of our consumers and keep them safe?” For Parizo, it was one thing to breach a card or retailer, but breaching a bureau like Equifax was of a different order. A bureau takes responsibility over the consumer by monitoring their creditworthiness. So who should be monitoring the monitor?

For Vaduvur from Ondot, the answer was a more democratic approach: “Eventually the buck stops with the end user… our perspective is that the only way out is to give consumers better visibility and it's really security through engagement… There has always been a dichotomy between reaching out to the users and giving them too much power versus security, But now with new devices enabling ‘always on’ communication, higher engagement does drive higher security.” He gave examples, such as a notification to the consumer that their credit was being checked, plus the power to block it if it seemed suspicious: “if you have the visibility and you as an end user have the control, it might not solve the breach, but it could certainly mitigate it.”

Mukherjee balanced that with the complementary need for central control. “I think what we are missing as a country is the enforcement of a data security standard, which many countries in the European continent have been able to establish and been able to enforce.

The establishment of data security standard, or a national data security standard, and enforcing that across organisations that handle personally identifiable information, is going to help monitor the monitors."

Having spent some time on the broader principles, Parizo turned the discussion back to actual security technology – this was, after all, a technology innovation conference. For example, the success, or not, of EMV's (Eurocard, MasterCard and Visa) move to chip and PIN smartcards: "where the payment cards themselves have embedded microchips in them that encrypt the payment data with the idea of fostering end-to-end security from the point that a card is presented for payment all the way to the payment processor and ultimately the banks."

The panel admitted that we again face a dichotomy between the user experience, and the trust in the processes going on in the background. As Schiff explained: "typically people only have one mortgage, one cheque account, but often have several credit cards. So it's a very different competitive dynamic."

Applying for a bank account, one accepts a certain amount of hassle: if the bank requires a lot of security checks and personal details, the applicant accepts that they are probably doing a thorough job. But if a new credit card purchases are hedged by tiresome authentication procedures, the card will be moved to the back of the wallet. "At the point of sale, there's no question the transition has had its challenges. I think we've all waited 10 or 15 seconds in some cases for a transaction to process. I guess it must sound a bit spoiled when we complain about waiting 10 seconds to process a transaction, but I think everyone recognises it's a source of frustration."

Another irritation, pointed out by Parizo, is the confusion about whether to swipe or dip the smartcard. Haven't we all had the experience of a waiter or counter clerk trying first one and then the other before getting the payment accepted?

These may be very minor frustrations, but they have a cumulative effect when daily payments are being made for groceries, meals and minor items. Individual card issuers cannot do much about these delays, because they are caused by the network rather than the card, but they could be providing a big boost for contactless NFC (Near Field Communication) digital wallet systems, such as ApplePay, being offered by the phone companies. Ultimately what matters is the security of the system, but the user experience is what will shape usage patterns, as well as the competitive advantage of the financial service provider. So how well is NFC performing now?

Schiff suggested: "As a rule of thumb, we tend to say that in order to get people to change the way they pay, the new payment mechanism has to be 10 times better than the prior one. My guess is Apple Pay is two or three times better, not 10 times better." It is certainly good not to have to key in a whole credit card number, so it looks like the real differentiator will be how easy it is to load the card details into the digital wallet: "There are two things that strike me. One is in almost every case it's a pain… you've got to go through several steps, potentially call your institution. The second is there's a surprising amount of difference in what institutions require you to do to authenticate and identify yourself so that you can load

your card into one of these wallets. As those things standardise and get easier, I think we will see many more customers trying out these services."

We were reminded by Mukherjee that, however simple, it it always takes time to win confidence. Plastic cards themselves were very slow to be accepted at first, as was ACH (Automated Clearing House) for fund transfer. But once accepted, they became essential. Ron Green reminded us about the inevitable inertia of a massive customer base: "In other countries, particularly where digital economy is not sufficiently pervasive, you have the luxury of being able to do a top-down governmental program. I don't think that will really work in the US… So I think the innovations have to come from the edges, the retailers and the issuers, and that's really what's happening."

Ondot's Vaduvur pointed out that you need to add real benefit to change ingrained habits. Talking to end users about mobile wallet offerings and what they really cared about, his company had been asked: "why the hell should I pick up my phone when I already know how to use my card? What additional value do you offer? If all you're doing is changing the form factor, it's only marginally useful." Some 42% of people surveyed in the US said they were not comfortable using a phone as payment, so the real emphasis should lie in adding value or making significant improvements to the user experience. What can differentiate one card from another is the ease of activation: when a replacement comes, can you go out and use it? Or do you have to phone, answer security questions or log on to a computer before it can go into your wallet?

Parizo asked for concluding statements on the future of FinTech Security. Green mentioned EMV's move to embedded chip smartcards and added: "We will continue to do more to advance security; if you look at our ID check solution where we're using facial recognition to allow for a transaction to occur. But we're doing other things like behavioural analytics or device identity checking; we're making those capabilities available to our customers so that they can be more assured that the security of their transaction is being well maintained." Schiff and Mukerjee both invoked Big Data and AI to pull together the vast amount of data that is now available, especially via the Internet of Things (IoT). Mukherjee expanded it as: "at Technology Credit Union we have plans to do even further, is to analyse and bring in machine learning and leverage the data that we already have on consumers and then be able to predict and even prevent any fraud and even enhance the ultimate experience… that's the direction that everybody is going, and I think this is the natural path for financial institutions to take to enhance member experience."

Vaduvur took a contrasting stance: "The short answer is empower consumers to take control. If I can control when, where and how my payment instruments are used, where my card is used and I have instant visibility and if I have control, then I'm more engaged, I use that card more, and that means collateral benefit for the issuer."

It was a fascinating comment, because Vaduvar was representing Ondot, a company that provides just that sort of control to cardholders. As their literature points out, the card issuers are up against formidable intelligence: the intelligence of hackers, of cyber criminals and industrial espionage. But there is a vast fund of intelligence that they are not exploiting to the full, and that is the combined intelligence of their customers. For all the power of big data and AI, no one yet knows individual spending habits better than the individuals themselves. So there could be huge security benefits from a simple interface that allows the user to

instantly control how the card can be used – in what locations, at what establishments, for what sort of purchases at what time – and allows immediate notification of its use.
Green commented: "…securing the credit or debit card based on the location per transaction or number of transactions, depending on the proximity to where you are. That's a great innovation." He added: "From the issuer perspective, I think the biggest thing is to make sure that, number one, the data itself is secure and there are effective fraud management systems. But, going back to co-opting, the consumer: that's the fastest way to figure out whether fraud happens or not."

Central intelligence, or the distributed intelligence of the user base? Either way, the discussion ended on a hopeful note. And I especially appreciated the way it had pulled together so many factors impacting FinTech security strategy: not just the machinery of technology versus the invader, but the importance of user experience in a competitive market, perceptions of security and the potential role of customer engagement.