MAGTEK®
SECURITY FROM THE INSIDE

On September 26, 2011, the Federal Reserve Bank of Chicago and the Secure Remote Payment Council cosponsored an invitation-only symposium focused on security issues for remote payments. During this complimentary event, thought leaders from throughout the payments industry, law enforcement, academia and government convened to discuss issues related to Internet, mobile and card not present payments.

The following is a copy of Mimi Hart's speech on fraud mythology in the payment world:

Thank you very much for being here today and for the privilege of allowing me to present some ideas on certain myths that exist in the payment world regarding fraud, and certain "false gods" that play a role in the fraud mythology.

The first is the myth of "the cost of doing business". We all hear this expression regularly - that fraud is manageable, that it's tolerable and it's just the cost of doing business. Well whose cost is it really? When fraud strikes big, we're NOT in this together. If you get hit, it matters little if fraud losses "on average" are improving or worsening.

The pain of fraud is not proportionate. We measure it in the aggregate, but you can only see the impact when you look at the spikes on the graph. Consider Heartland or TJ Maxx or Sony. They could take little comfort at the time of the breaches that payment card fraud could be expressed as a few basis points "on average." We may work together, but when fraud strikes we suffer individually.

Risk of fraud in card-based payments cannot be hedged. No one indemnifies participants in the system as it is, other than consumers who we all agree can and should get a free ride (sort of) if you don't count hours wasted, lost wages, worry and aggravation. That's a penalty for fraud that we rarely quantify.

Next let's ask, if this is the "cost of doing business" - whose business are we talking about? Issuers and retailers allow security protocols in their own shops over which they have little control. But worse yet, these protocols have yet to prove effective at the level of the breach.

We are told that nearly 60% of all retailers and processors are PCI compliant, but daily we hear word of new breaches, large and small. Can we truly blame this on sloppy retailers, or complacent issuers, or blind eye auditors, or have we considered the possibility that the specified protocols are just plain ineffective. Do we understand the problem? Have we done a root cause analysis? Or have we been lulled into a state of false confidence with the blessing of a false god.

On the other hand, new entrants in payments do not respect the legacy environment. "Just because" is an answer falling on deaf ears. These entrepreneurs use the retail and wholesale payments industry any way they can get away with, rules or not. Just look at Square.

As legacy players, we find ourselves in the proverbial "between a rock and a hard place." Your board of directors won't care that you followed PCI. You will still be fired. An entrepreneur's Board of Directors can't spell PCI.

PCI is one of the more dangerous "false gods" in payments.

The PCI Security Standards Council is not a standards making body by our industry's definition. It makes rules. It is not inclusive, nor consensus building, nor open like ANSI and ISO. It has an advisory board that is informed what new rules were made last week - just before they're announced to the public.

PCI is a private rules company with a very pious persona. The PCI DSS is not a standard, it's a strategy. It is an agent of the brands, who are its owners. It exists solely to serve their needs. Make no mistake about it. Its stated mission is to protect cardholder data, but its true purpose is to delay, deny, deflect and distract. It is the ultimate preserver of the status quo and a serious obstacle to innovation.

It exploits the relative weakness of the merchants, vendors, and processors. And it does this - all in the righteous name of "consumer protection". This fox in sheep's clothing has no interest in curtailing fraud. After all "No Fraud" translates to "No need for PCI" and do not forget - this is a for profit enterprise. Remember too that the brands make money on every transaction, fraudulent or legitimate.

The same organizations that set the interchange rates, make the PCI-DSS rules, and enforce those rules with the power to levy steep penalties and fines. That's somewhat like the power to be judge, jury and executioner all rolled into one. Is there not something wrong with this picture?

PCI has rapidly become a self-perpetuating, self-aggrandizing, profit motivated authority. It has and will continue to stifle innovation by its often nonsensical rule making. First it takes a lowest common denominator approach to technology assessment. Let's use the latest announcement on encryption as an example. At MagTek we began manufacturing a new breed of reader back in 2005, before PCI had been created. These readers had multiple layers of security including encryption, token generation and authentication built into them. We call them MagneSafe and we have delivered a half a million of them into the marketplace.

We have also worked for the last two years with many industry players on an ANSI standard for encryption. As of last week, PCI has announced that all magstripe readers will soon be subject to new rules and bureaucratic certifications. In other words, now all reading hardware will require the PCI blessing from a certified PCI lab. You may think this is a good idea but it is actually ridiculous.

The cardholder data on a magstripe is in the clear. It consists of a bunch of zeros and ones. It is a machine readable magnetic barcode. Twenty of the characters it contains are printed or embossed on the front of the card. The other sixteen characters can be viewed just as easily. They are not secret.

Encryption, no matter how strong, cannot protect data that has already been written on the blackboard. The serial number on a twenty dollar bill cannot be protected with encryption, because anyone can read it. And so you might say, well not everyone can read the data on the stripe, so let's add encryption to protect it. If you think of the data on the magstripe as written in braille rather than binary code, just because you can't read braille does not mean the data is safe.

Why should merchants and processors be forced to protect data expensively and needlessly? It starts out in the clear on the card and it ends up in the clear at the brands, but in the middle it's your responsibility to shroud it. And now PCI will dictate just exactly how to do it!

We know how to protect the card data and PCI doesn't or I should say they do know but choose to look the other way.

You must understand - PCI is not about fraud reduction or cardholder data protection. Compliance is the name of the game. That's how you are measured – not by fraud reduction.

Two years ago PCI presented a report that that had been prepared by Price Waterhouse Coopers. It touted encryption and tokenization to aid compliance and reduce scope. That same report said certain technologies had the potential to reduce fraud and even "eliminate the need for PCI", but has PCI even considered promoting the technologies that could render themselves useless - The answer is simply NO.

Cardholder data is but one element of a safe and secure payment system and it can only be protected by strong authentication. Encryption is a distraction.

But it is not the only element that needs protection. Endpoint authentication is an answer to the six essential elements of a secure transaction.

The first is the payment instrument. This can be a card, a phone, a fob, or some other device. We need to know with certainty that it is genuine and not a clone.

Second is the data it carries. We need to know that it has not been altered. This might be the account data, but it need not be.

The third is the bearer. The user must contribute a piece of knowledge to the authentication process.

The fourth is the terminal that accepts the data. We need to know that it is also genuine and has not been tampered or substituted.

The fifth is the recipient of the data and the intermediaries. We need to be certain that the data travels through legitimate pipes and reaches the rightful host.

And the sixth is the details of the transaction. If I intend to pay you $100 dollars, it can't be modified to $1,000 somewhere in the process.

When we can authenticate those elements of a payment transaction we can have a truly secure system, whether face to face or remote transactions.

At MagTek we offer such security. We rely on open standards and sound security principles. Our payment technologies revolve around multi-factor authentication – something you have – a unique object that cannot be counterfeited, something you know – a PIN, a password or a secret and always something else - something unpredictable. In our case, we read the unpredictable value off of an ordinary magstripe card.

Any authentication method needs to incorporate dynamic data. All static data is vulnerable. It can be read, copied and reused. This is the root cause of our skimming and database breach problems. When we only rely on static data, we can't determine if the data on the card being presented was stolen from Sony's database or copied at a skimmer on an ATM.

But if a dynamic or one time use property can be added to the authorization process and authenticated, then the stolen static cardholder data becomes useless to the criminal because he has no means to predict or generate the next authentication values.

It is industry standards that have contributed to the ubiquity and success of the magstripe card, but those same 40 year old standards put a stranglehold on magstripe security and give it an undeserved black eye.

IBM tried to change the Track standards back in the 80s and met huge resistance because even then, the payment structure had become very rigid. The technology has progressed greatly. Magstripe cards today can store thousands of bytes of data. Not just the track 1&2 data we know. And modern readers can read hundreds of extra bytes of data that emanate from the stripe itself. These extra bytes represent the magnetic signature of the card itself. And they have a remarkable quality, they are stochastic by nature. That is they change unpredictability with every swipe but within boundaries by which they may be correlated and authenticated. The magstripe card itself is not insecure, only the readers need updating.

Which brings me to the next "false god" - EMV. The promise of EMV is dynamic authentication, but….

EMV is a 25 year old protocol for so called smart cards, which is a cute term for a microprocessor embedded in a piece of plastic.

EMV cards are expensive to issue - five to ten times the cost of a magstripe card. They are expensive to process and will require massive changes to our payment infrastructure – which will take years to implement and billions of dollars. Merchants will need to purchase new terminals at their expense. Consumers and merchants will need to learn new behaviors.

And after 10 years or more what will we have? A card that is still susceptible to cloning. It's just a little piece of silicon, like the processor in my laptop.

For security, it relies on complex key management routines. These routines fall under human *process control* which we all know can breakdown rapidly. We have trouble enough with managing keys between terminals and acquirers. Now envision managing keys on every card you issue and ensuring interoperability on every terminal the card may interact with.

Chip cards were originally meant to solve communication infrastructure problems between countries. Remember when it used to be nearly impossible to call Germany from France? Chip cards to be effective today, require online authentication. Ask the UK card issuers who have now reissued their chip

cards three times – to move from static authentication, to pseudo dynamic authentication, to online dynamic authentication.

There are still known flaws in offline PIN verification. The EMV cards are also fragile. The chip can be destroyed by microwave, by a ball peen hammer, or simply bent or broken in your wallet. They're costly to issue and costly again to reissue.

There is little dynamic data, a three character CVV is all there is between you and the criminals. The PAN is still in the clear, which means PCI still applies. And what value will the US version of EMV bring to e-commerce fraud? Without a PIN, the user cannot be authenticated. So the cardholder will have a much more expensive card, but one that still carries the PAN, so keeps the merchant in scope of PCI, and adds not a shrivel of security to the on line purchase.

I am not against CHIP and PIN, but I do question the business case and the need to so radically change a payment system that "on average" functions quite well. If the world wants EMV, I say bring in on. It will be good for business. But respect its limitations. If it's dynamic authentication you're looking for, there are far less expensive ways to get it and use it.

Try as some might to kill the magstripe card, it will be around for decades to come. Gift cards, prepaid cards, loyalty cards, reward cards and secure payment cards all will bear a magstripe. So no matter the investment you make in EMV, it is foolhardy not to protect the magstripe simultaneously. Why put an expensive lock on your front door and leave the back door wide open?

Our last myth to bust today is the myth of "the Chicken and the Egg".

Because we operate in a multi-constituency environment, many people believe that we must follow a ***centrally dictated*** path or we won't be able to deploy security effectively across the system. This is nonsense.

Almost all effective fraud control today is not applied or paid for across the system, but at the endpoints: retailers and issuers working hard to protect themselves. Why? Because control across the network, with its vast connectivity and plurality, is an illusion. So, we need not try to boil the ocean.

And, we don't all have to jump into the same pan. We need to be able to select our solutions tactically from a free and competitive marketplace to solve problems specific to those at hand. For example, in the remote space we need solutions to combat man in the middle and man in the browser attacks. We don't see the same issues in the brick and mortar world.

A history question: forty years ago, if magnetic stripe payment cards were the eggs, what was the chicken? I'd suggest it was magstripe payment terminals. How about ATM networks and PIN at POS. All of these were pioneered by a small group of influential, but certainly not omnipresent, organizations who had a vision. They found ways to lay a few eggs, and round up a few chickens.

We did not need a benevolent dictator to make automated payments happen for us back then and we don't need one now. Payments is not a banana republic. We should not bow down to the false gods. We should ignore the dictators, or depose them if necessary.

So…what's next? If you are an endpoint, don't wait for authentication security to come from above, start implementing it yourself now. There are plenty of solutions in the marketplace that have the ability to prevent, detect and better yet **disrupt** fraud in real time. If you don't know where to begin looking, could I suggest you please start with MagTek?

Thank you for listening.

Annmarie D. "Mimi" Hart
President & CEO
MagTek, Inc.