The Story of Little Billy Waldron

and the Unfortunate Exposure of Cardholder Data

by: Amelia Waldron

January 2013

All names and persons referenced herein are entirely fictional.

The summary to the jury

Ladies and Gentlemen of the Jury, thank you for being here today to render your verdict on this important case before you. The question you must answer today, now that you have heard all the evidence is:

Was Sincerra Payment Systems at fault for its handling of cardholder data?

Surely, the personal data of nearly 100 million cardholders was exposed to criminals. We know these criminals have already used some of this information to make counterfeit cards and defraud countless victims and we do not yet know how many more victims will come forward as time goes on, as many of the real criminals remain un-apprehended. Yet, today you must judge Sincerra.

We have shown you that Sincerra was an extremely conscientious company that followed all the rules to protect cardholder data. You know that it also went to the time and effort to have regular audits by independent firms to make sure they were doing everything possible to secure their network and their systems. You heard testimony that they were considering "end to end" encryption systems, but they had seemingly been slow to act on implementing these stronger, more protective measures. The plaintiffs have suggested to you that had Sincerra implemented this type of encryption sooner, which was not an industry requirement at the time, they would have spared themselves this trial, the angst of their customers and the steep fines and penalties now looming over their business. But we have shown you the fallacy of that logic. You the jury have seen for yourselves how little encryption would have helped them, even if they had implemented it throughout every inch of their network and servers.

And you have come to see the real culprit here. You know in your hearts that this is a good company done in by a bad system over which they had very little control. I ask you to ponder for a moment:

- Who really caused this problem?
- Who put these hundreds of millions of cardholders' identities at risk?
- Was it Sincerra?

The answer is absolutely, positively, NO. We have proven beyond all reasonable doubt that it was not Sincerra that caused this suffering. It was in fact the card issuers who put their clients and their clients' identities at risk. The evidence has shown that the cards were insecure when they were first delivered to the consumer. The information embossed and printed on the cards can be read by everyone and the information recorded on the magnetic stripes can be read by anyone who spends a few minutes and a few dollars to examine them. They are not at all secret. Binary code is not a secret language. It's taught to our fourth graders. The barcode on a box of Cheerios does not contain secret data. It's used for automation - and no credible data processor would tell you that a barcode is secure. It's purely a tracking number that can be scanned at the check out counter, to make your purchase a little quicker and easier and to help a retailer re-stock the shelves more efficiently.

As we have shown through weeks of evidence, the magnetic stripe card was intended to offer the same convenience.

But something happened along the way. The data embedded in credit, debit and ATM cards became far more valuable to the crooks than the barcode on the Cheerios. For years now, the criminals have been reading the card data, and transferring it to other pieces of plastic. This is known as “skimming fraud”. Once these thieves get the data, they make counterfeit cards and rob people like you and me, and merchants and bankers and processors and the card issuers. For many, many years this has been going on, but did the banks and card issuers do anything about it? No. You have heard much testimony that they considered this type of loss to be “an acceptable cost of doing business”. We the public suffer, but they judge it to be an acceptable loss. Does this sound like the same argument that we heard about seat belts and Pintos? How many exploding wallets and bled out bank accounts do we need before the card issuers add some necessary safety to their products?

You will no doubt remember little Billy Waldron. He spent just a few hours on the stand, but in the course of twenty minutes he read the encoding on 12 magnetic stripe cards. You watched as the judge handed him a card from his wallet, and you heard the judge assure you he had never shown his credit card to Billy Waldron before the moment of his testimony. Then you watched as Billy sprayed a developer solution on the magnetic stripe and used a white board to write down about 200 zeros and ones. Remember that spray you saw, it costs about $25. Then you watched as Billy quickly parsed out the zeros and ones into groups of five, and then he called out and printed on the white board every number on the magnetic stripe. He read the Judge’s account number, his expiration date, and his magnetic CVV information, and then just to prove that this wasn’t a fluke, he read 11 more cards that even some of you volunteered from your wallets.

Right after that Detective Pierce testified. He brought with him a card reader that he plugged into his PC and he read the same 12 cards again. It was much faster than little Billy, 12 swipes took him about half a minute. But when he compared the output from the card reader to Billy Waldron’s hand written card information, it matched every time; Little Billy was 100% accurate.

Now what did we learn from this testimony and evidence. First, card data is easily readable. Billy Waldron is not a genius. He testified, under oath, that he was a B+ student, in the 86th percentile of his class at Pleasantview Elementary school. He happens to love math. His math project in fourth grade was to demonstrate his knowledge of base 2 versus base 10. Billy can read base 2, zeros and ones, as easily as you and I can read decimals. He is not a criminal. But technically he “breached” your card data. He exposed it for you to see. He put the information he read from your cards up on a white board. We printed it out and gave you copies that you will recall are marked as Exhibit D. We did not encrypt that data before we gave you the copy. Billy and I broke the rules of PCI-DSS, but who wrote the rules and why must Sincerra protect this data so vigorously, when little Billy and I can read it so easily.

Yes, Sincerra had a data breach, they admit it. But, let's consider what Sincerra had done to try to protect your data. When it was on their servers, they encrypted it. But a hacker broke in to their network and installed "sniffing" software, so that they could get the data before Sincerra had a chance to encrypt it. And I know you asked yourselves, why it was unprotected in the first place. Why could they not have encrypted it before it got to the "sniffer"? Well that's a darn good question and you heard the answer through the testimony of John Mathersby of MasterCard. He read the MasterCard operating rules and somewhat reluctantly pointed out 12 different places where MasterCard stated a requirement to, and I quote, **"to read and transmit the entire unaltered contents of the Magnetic Stripe."** When you go into the jury room this afternoon, please review the highlighted sections of the "MasterCard Chargeback Guide" - dated October 2008, which is marked as Exhibit K.

So now we further understand the Herculean task – that faced Sincerra. Follow the first set of rules which require that you keep the magnetic stripe track data in its "entire, unaltered" state until the point of authorization, but then make sure it stays safe from criminals after it's been authorized. How illogical are these rules? The first set imposed by the Card brands and the second set imposed by PCI-DSS. Now, please be reminded about just who owns PCI and who enforces the Data Security Standard. Yes, take Exhibit Q with you into the jury room and review that PCI is owned by the card brands, namely VISA, MasterCard, Discover, American Express and JCB. It's a profit driven business that tells the merchants and the processors what they have to do to protect cardholder data and then its owners dole out fines if criminals "breach" the payment system before or after the point of authorization. Any good thief knows to install the "sniffer" software before the point of authorization, where it's required to be in the clear, so what is the point of encrypting it afterwards? And don't forget even 10 year old little Billy can read the cardholder data.

Now, Ladies and Gentlemen of the Jury, I ask you again why the card issuers did nothing to protect their cards. If I give you the key to my front door, should I take steps to make sure that you cannot make a copy of the key? Yes, I'm going to buy a key that's really difficult to copy and one that carries a label "DO NOT DUPLICATE". But then again maybe I should just do what the card issuers have done. If my house is broken into, I'll blame you for not storing my key adequately. I'll say the key was easily copied by a burglar because when I gave you the key you took a picture of it, put the picture on your PC and did not encrypt the little grooves and ridges. If you had protected the image of the grooves and ridges on the key, my house would not have been robbed, so therefore you are responsible.

The banks need to issue a better key, and one that they can recognize and know that it is legitimate and not a counterfeit. These data breaches occur for only one reason, the thieves want the data so they can make counterfeit cards and steal money. Sometimes they use the counterfeit cards to hack cash from an ATM and

sometimes to buy expensive items that they can fence for cash. Either way they are stealing our money, but forcing processors to encrypt the data subsequent to authorization will not stop the fraud, it will only help to contain the scale of the breach. Little Billy can still read cards and criminals will still be able to purchase or build a reader just like the one Detective Pierce showed you. So the data collection will take a little longer but will be just as usable to hack an ATM or purchase a $3,000 flat screen TV to fence.

WARNING: COUNTERFEIT CARD IN USE

And who needs to breach a processor that stores "millions of transactions a month"? During this trial you also heard about RBS, another processor that was broken into or as we say "breached". The criminals used only 100 cards to steal $9 million dollars in 30 minutes. Detective Pierce showed you his database of cards that he personally had read. He had more than 500 cards, which had taken him slightly more than 3 weeks to collect. And he was not gathering data surreptitiously. If he had a side job in a restaurant or a gas station or a bank, he could probably have collected thousands of cardholder data records in that time.

There is only one major difference between paper money and plastic money. The paper money has anti-counterfeiting features built in. The Secret Service can examine a counterfeit twenty dollar bill and know that it's a fake. The card issuers could do the same, but they don't. The card issuers could protect that data on the magnetic stripe, but they do not. The card issuers will tell you that fraud is not that big a problem, that it's manageable, that it is just a cost of doing business. Some card issuers even joke about fraud. They have funny TV and radio commercials, or annoying jingles about fraud and identity theft. They tell you not to worry if your bank account is wiped out because they'll stand behind you and "put the money back". So, I ask you, why they would not invest in card security and stand in front of you?

Why not put a good lock on the door? Why should they not be able to spot a counterfeit card and make it unusable? The technology exists, but they don't use it. Why? The answer, Ladies and Gentlemen of the jury, is painfully clear; because it is easier and less costly to blame somebody else; sometimes the merchants like TJ Maxx and sometimes the processors, like Heartland or now Sincerra. It's never their fault. In fact they whine and complain to the media and the Courts that they had great costs to re-issue the cards and provide credit monitoring to their cardholders. Yes, there's a great moan and gnashing of teeth and then they re-issue another card with a new account number... that Billy and I can read and copy.

You would think they might have heard the old expression, "Fool me once, shame on you. Fool me twice, shame on me." How many times will they need to re-issue cards and whine about it, before they finally decide to take action and protect the data on the card they issue? Wouldn't it be nice to see the authorization system say –"Sorry that card was declined because it's counterfeit"? Instead, the card issuers rely on you and me to

open our statements, tremble with fright when we see a zero balance, and know it's our responsibility to report the fraud, sign the affidavits, take time off from work, make a zillion phone calls, and all because the card issuer did not use any anti-counterfeit features on their cards that could be read at ATMs and the point of sale.

You heard the testimony of several card experts. They testified about several anti-counterfeit options that were available to the payment community. You heard new expressions about counterfeit recognition methods and lots of statistics and you saw for yourselves how technology could have been used to detect counterfeit cards and shut down the fraud. Detective Pierce showed you a tampered card and a real one, and then he showed you how to spot the fake one. Remember the demonstration, when you saw Detective Pierce read off the verification values. He pointed out that they changed dramatically with every swipe, but nevertheless, he was able to tell which was good and which was counterfeit.

When this trial is over, you can forget those complicated words, but today I ask you to remember Ms. Cheney who described a bona fide path to cardholder data protection. She used RBS as a great example when she said, "End to end encryption will not prevent fraud. It is helpful to contain the size of a breach. Only when card data encryption is combined with strong authentication can it protect the cardholder. It is the authentication piece that can protect the cardholder in spite of a breach." Little Billy could have read the data from the 100 cards used in the RBS attack in less than a day. But if card authentication had been used in the ATMs, the banks would be $9 million dollars richer today – and the thieves would be $9 million poorer. As Ms. Cheney testified "Encryption makes it difficult to steal the data, whereas card authentication makes it difficult for thieves to use the data and profit from the crime. If you want to protect the cardholder, you need to have both."

Then Mr. Fernandez, another security expert testified,

> *"In the world of crime, if you reduce or remove the profit factor from the equation, you remove the incentive to steal."*

So he concluded that although he would always prefer to use both encryption and authentication, if he could only have one – it would be authentication. Let me quote him.

> *"I'd rather stop the payout, than stop the data theft. As a fraud fighting tool, as a consumer protection tool, I can say that card authentication is decidedly stronger than encryption."*

TAKE THE PROFIT OUT OF CRIME.

PREVENT THE PAYOUT

And please pay close attention to the instructions you will hear from the Judge before you begin your deliberations. He will define again a legal term called "the standard of care". If merchants and processors are forced to be PCI compliant and must spend a great deal of time, money and inconvenience in order to protect cardholder data, why is the "standard of care" required of them so much greater

than the card issuer? Remember the card issuers set the "standard of care" when they mailed the cards to you and me. They published an industry standard, a document that taught little Billy and me how to read the cards, but now they are righteously indignant that Sincerra did not prevent criminals from seeing the data on them, and they say that's negligence. If the data is that precious, that it warrants an elevated "standard of care" surely the negligence began the day the card was issued. I tell you, it's ludicrous to produce a card with data that the entire world can see and then insist that it's sensitive and must be shrouded in secrecy by anybody else who comes in contact with it. Essentially the card issuers, abetted by the brands and PCI, have told the world, "we don't have to protect the data, but you do."

So let us look again at Sincerra, are they guilty, were they irresponsible? No, not at all. We have demonstrated by truthful testimony and credible evidence that Sincerra not only acted with a great sense of responsibility, and a determined effort to protect cardholder data, but we have also demonstrated that the card issuers knew or should have known how to protect cardholder data with counterfeit recognition measures. But instead they intentionally "passed the buck" and relied on PCI-DSS to obfuscate the actual problem. Please send a strong message to the hypocritical financial institutions, the aggrieved parties who have brought this suit against Sincerra Payment Systems. When even little Billy can read the data, be honest, and ask how was Sincerra realistically supposed to safeguard it? Please render your verdict and tell the world that Sincerra is not the liable party.

UPDATE:

The jurors deliberated for less than one hour.

They returned a verdict of
"NOT LIABLE" on all 37 complaints.

Lawyers for the plaintiffs have said they will appeal.