



Off the Press - January 2009

PENNSYLVANIA ASSOCIATION OF COMMUNITY BANKERS

THE VOICE FOR COMMUNITY BANKING IN PENNSYLVANIA SINCE 1876

Could Banks Do More to Stop Debit Card Fraud?

By: *Jeremy Burris, CISA, MCP, CPTS, CEH, ECSA, S.R. Snodgrass, A.C.*

With debit card fraud on the rise, are banks doing enough to prevent, manage, and prosecute these crimes? An incident that recently occurred to me, personally, gave me new insight into the good, the bad, and the truly ugly heart of this “victimless” crime.

While traveling from our home in Pennsylvania to the West Coast, my wife and I attended a concert and bought a souvenir band T-shirt. When I was handed the receipt for my debit card purchase, I noticed that my entire debit card number was on it. My thought was, “At this point, they’ve got my entire credit card number on their copy so there isn’t much I can say or do about it now.”

When we returned home a week later we received a call from Visa’s Fraud Protection asking us to verify some recent activity. I was alarmed to hear a list of 11 recent charges that I had not authorized, all on the West Coast. After we spoke to customer service, Visa declined all but one of the charges. These ten had been held pending authorization because the user did not have the three digit security code or other personal information to verify the card number. We still don’t know how the single purchase that was approved got through.

My own bank later confirmed that all but one of the charges had indeed been disapproved.



I completed a dispute form and was credited within two weeks for the single charge. My account was also charged \$50, which was later refunded as well. Altogether, there had been \$1,100 worth of attempted charges on my account.

LACK OF CRIMINAL FOLLOW-UP

I contacted the state police, who asked me to complete a “Victim Report.” They informed me that they would NOT be taking any action because the amount of money lost was only \$50. Since I had spoken to the vendors involved, I knew there was information that could well have led to an arrest. The state police told me I could contact the local branch of the FBI but that I would probably meet with a similar response.

While my own losses were minor, the total potential losses from this scam could well have been in the millions of dollars, if

you consider there were some 30,000 people at the concert that day. How many of them were also ripped off, and how many of those charges were approved? Moreover, the thieves gave a shipping address that could easily have been followed up on. And the source of the card data was clear. Nevertheless, the crime was never investigated, much less prosecuted.

THE GOOD:

In the end, I got a new card, the refunded \$50 fee, and immediate credit for the \$1,100 worth of attempts that had memos posted to my account. So, Visa fraud protection did a good job of determining what might be a “suspicious transaction.” None of the purchases that I actually authorized were put on alert, only those that truly were fraudulent.

The following controls were in place (and they worked) to reduce the likelihood of this happening to a customer:

- The Visa framework – the Visa fraud protection correctly identified the suspicious transactions and put them on hold
- The Bank – controls were in place to help identify and refund fraudulent charges
- The consumer (in this case, me) – for responding quickly to the incidents

From a Bank’s standpoint, if



Off the Press - January 2009

PENNSYLVANIA ASSOCIATION OF COMMUNITY BANKERS

THE VOICE FOR COMMUNITY BANKING IN PENNSYLVANIA SINCE 1876

they have already partnered with Visa and have internal controls for investigating fraudulent transactions, the only other thing that can be done is to educate the consumers who carry their cards.

THE BAD:

It is hard to believe that any card-processing device would still include the entire card number on the receipt. The bank that processes the merchant's card receipts is clearly at fault here. After all, the consumer is in a bind. If you tell the vendor you are not comfortable with the entire card number on the receipt, they can reverse the transaction—creating a second receipt with your entire card number! Really from a consumer (or cardholder's) standpoint,

the only thing that you can do to prevent this type of thing from happening to you is to ask EVERY vendor PRIOR to handing them your card if they print the entire card number on the receipt. If they say they do, pay with cash; otherwise, you run the risk of a vendor getting your entire card number on paper when you make transactions.

THE UGLY:

Police authorities would not investigate because of the small amount of my personal loss. But the criminal activity was potentially very large—as was the potential liability to the banks involved and their insurers. Financial institutions need to push harder to make sure that these

types of crimes are investigated and prosecuted.

In the end, the incident taught me that our controls are far from flawless and that more needs to be done by way of education and testing of incident response plans as controls against fraud.

ABOUT THE AUTHOR:

Jeremy Burris is a Senior Technology Services Consultant at S.R. Snodgrass, A.C. Jeremy's areas of expertise include Network Attack and Penetration and other IT security-related audits for financial institutions and private companies. Snodgrass is best known for our expertise in the financial services industry, where we currently serve over 175 financial institutions on a national scale. Accordingly, we have extensive industry business experience and sound working relationships with all of the regulatory agencies. Examples of that experience are displayed on our Web site's Knowledge Bank at www.srsnodgrass.com, where you can view several articles and video presentations on banking-related topics, including a live Attack and Penetration demo.