

SECURITY BREACHES AND THEIR IMPACT ON OUR INDUSTRY

By Paul A. Rianda, Esq.

Protecting personal and credit card data has become a hot button topic in Washington and many state legislatures, because of numerous security breaches at personal data warehousing companies and credit card processors. In this article, I will provide an overview of the reason that increasing numbers of these security breaches have occurred, the framework that the credit card associations have implemented to deal with the issue and the potential ramifications of these breaches on our industry.

Why The Increase in Security Breaches?

Over the last few years, due to the expanded use of the internet and the subsequent accumulation of personal and credit card information, there have been a number of spectacular data thefts. Many large databases of information have been gathered by private companies such as credit reporting companies, as well as numerous credit card acquiring and issuing companies. Prior to the advent of the internet, these databases were usually fairly secure, because it was difficult for individuals who were not employed by the entities to obtain access to the information. Therefore, before the internet gained widespread use, the focus to secure the information databases was primarily on trying to ensure that employees did not take the information. Thus, this limited the scope of security efforts and made the job of securing data much easier.

With the advent of the internet, access to information has become much broader. The internet can be utilized to allow people access to information in a much more efficient fashion and has become a major market place for buying and selling goods. Credit card processors now process transactions over the internet and credit reporting agencies have made credit reports available on the web. These organizations allow access to their databases through the internet to allow more convenient access for their customers, partners and employees. However, this leads to a situation where not only partners and employees, but potentially criminals and other bad actors that wish to misuse this information can also obtain access to the data.

Over time, these security breaches have become increasingly larger and therefore more alarming. A number of years ago, there were some initial breaches through merchants and even through credit processors such as Creditcards.com. However, these breaches were not as significant as those that have occurred recently, such as at Card Systems, wherein it is alleged that 40 million credit card numbers were potentially compromised. Also, recent breaches of security at AOL and Choice Point have served to focus a spotlight on this issue and bring it to the national political arena. Congress and most state legislatures have seized upon the issue due to the heightened publicity of the issue and are proposing legislation to regulate the security of databases that had previously been monitored by private companies such as Visa, MasterCard and the credit reporting agencies. In addition, these proposed laws would impose a requirement to provide notice of any security breach to persons who potentially could have had their information stolen.

Industry Attempts to Safeguard Data:

There have been industry attempts to try to minimize the potential for security breaches. Visa and MasterCard jointly promulgated their Payment Card Industry Data Security Standard (“PCID standards”) in an attempt to try to keep any further breaches from occurring, or at least minimize the potential for future breaches. The PCID standards are set forth as a set of standards that must be complied with in order to allow credit card processors, merchants and the others with access to credit card information to process and store information required to process credit card transactions.

The PCID standards are to a large extent common sense necessary to secure any type of computer network. Some of the items addressed by the PCID standards are: how to protect stored data (including encryption of data), the use of updated anti-virus software, developing and maintaining secured systems and applications, restricting access to data on a need-to-know basis, providing each user a unique identifying code, restricting physical access to cardholder data, tracking and monitoring access to network resources and card holder data, regularly testing security systems and processes and maintaining a policy that addresses information security.

The ability of the card associations to prevent any further security breaches through the use of the PCID standards is open to debate. Visa and MasterCard have approved a number of different private companies to perform audits to certify various credit card processors and merchants pursuant to the PCID standards. The problem with the PCID standards is that although a company may be compliant with the standards when the audit is initially performed, there are apparently insufficient safeguards to ensure continued compliance as evidenced by the Card Systems breach. The question now becomes how will the credit card industry address this issue in order to lower the risk of additional breaches?

The Impact of Breaches on the Bankcard Industry:

The credit card associations and banks have been less than willing to cancel credit card numbers that are compromised and issue new cards as a way of dealing with the theft of credit card numbers. There is a cost associated with canceling credit cards and issuing new ones that would have to be borne by the credit card issuing banks. In addition, there is the issue of inconvenience to the consumers who would have to have new cards issued. There is the fundamental question of whether or not consumers will have enough confidence to continue to utilize credit cards as a means of purchasing goods and services if they are continually having their credit card numbers compromised and new cards issued. This could be one reason that banks, Visa and MasterCard are unwilling or unable to issue new cards every time that such a compromise occurs.

In addition, there is the issue of who bears the loss when credit card numbers and data are compromised. The current environment places the bulk of this loss on merchants. Merchants who take fraudulent cards, especially over the internet, are generally held liable for the charge backs that occur. This shifts the potential loss to merchants, a group that is not organized enough at this point to effectively fight Visa and MasterCard on this issue. Consequently, with better organization and political lobbying, Visa, MasterCard and the association banks to-date have continued to be successful in their attempts to have merchants bear the bulk of the economic impact of compromises to credit card processing databases.

However, if congress and state legislators get involved, Visa, MasterCard and the association banks may no longer be able to minimize the economic impact of these breaches to them. There are a number of bills pending in congress and in the state legislatures to try to address these data theft issues. California has already passed a law that calls for notification to cardholders under certain circumstances if their information is compromised. This has led to many companies being much more forthcoming in acknowledging security breaches and notifying consumers when their credit card information has been compromised.

It appears that it is inevitable that there will be laws passed to address the duties and responsibilities of Visa, MasterCard and the banks where credit card information is compromised. It is just a question of how, and what format, legislation will take. There is the potential that, as requested by Senator Diane Feinstein to the heads of various credit card associations, in the event of a compromise of a credit card number, that number would be retired and a new credit card issued. This is probably the most stringent requirement that could be placed on banks and card associations. There are lesser requirements that could be imposed, such as notification to consumers and the establishment of a list of stolen credit card numbers to allow fraudulent credit cards to be tracked more easily.

As to the impact on the industry, it is clear that the standards that are currently in place are not working as designed. A dedicated and intelligent hacker can potentially compromise any database in spite of the PCID standards or any of the other security standards developed by Visa and MasterCard. The fact that such standards are widely utilized and published allows hackers the ability to study them and find ways to work around them. Also, when numerous organizations use the same standards, it leads to a situation where if hackers can compromise one database they may be able to find ways to breach others because the databases are secured in a similar manner.

As to the impact on the various independent sales organizations and credit card processors such as Card Systems, the implementation of more stringent data security measures and more frequent audit requirements placed on them will substantially increase the cost of operating such organizations. It seems inevitable that smaller organizations will be unable to afford to comply with more stringent standards. This will likely lead to a situation of further consolidations in our industry as only larger players will be able to afford to comply with Visa and MasterCard regulations. This will also make barriers to entry into the industry much higher. Besides having to pay for continued compliance with any new standards, an organization would have to show that it had the requisite systems in place before it could begin operations, which would greatly increase start up costs.

The impact on companies that are compromised remains to be seen. Companies such as Card Systems could conceivably be driven out of business if Visa, MasterCard or the acquiring banks were to issue fines commensurate with those allowed under the Visa and MasterCard regulations. Also, acquiring banks could conceivably take over the operations of such organizations in order to ensure compliance in the event that they unmask a significant security breach. However, the likelihood of any such credit card processor like Card Systems going out of business to the detriment of their agents and merchants is extremely remote. There is a large value associated with the merchants that they service and that value continues to exist despite any security breach. As has been seen in the purchase of Certified Merchant Services, even organizations that have a less than stellar reputation still have value in the market place. Consequently, merchants will continue to process, agents will continue to receive

their residuals and cardholders will continue to use credit cards for their purchases for the foreseeable future. The question becomes how will these continuing security lapses impact the overall use of credit cards and will consumers continue to be confident enough to utilize Visa, MasterCard or any other cards as their preferred method for purchases? Stay tuned.

* Paul A. Rianda, Esq. is an attorney who has specialized in providing legal advice to the bankcard industry for the past 10 years. For more information about this article or any other matters, please contact Mr. Rianda at (949) 261-7895 or via email at paul@riandalaw.com

** The information contained herein is for informational purposes only and should not be relied upon in reaching a conclusion in a particular area. The legal principles discussed herein were accurate at the time this article was authored but are subject to change. Please consult an attorney before making a decision using only the information provided in this article.