

There are some good data security lessons and best practices to take away from two data breach incidents that made headlines recently. The first was a massive breach at Epsilon, a company who does email marketing for over 2500 companies including Target, Best Buy, Kroger, Capital One, CitiGroup, where millions of email addresses were stolen.

No credit card data was stolen in this attack however; the primary fear is that there will be a big increase in what are called spear phishing attacks as a result. These are attacks where a bogus email is sent to an individual by what appears to be a company which has a legitimate business relationship with the person. That email often tries to get the individual to provide personal information to the fake company that can be used to commit further identity or financial fraud. The bogus email could also contain a virus or other malicious software. To prevent spear phishing, it is critical that you ***never respond to any email that requests personal information***, especially those that look like they might have come from your bank or financial institution.

A second point to take away from this event is that Radiant, our channel partners and our customers have valuable data beyond the credit cards that we process. Employee records and customer contact information are valuable data that criminals want to get their hands on. ***Make sure your customers know that sensitive data does not just pertain to credit card data.***

The second incident involved the Massachusetts attorney general fining a Massachusetts based restaurant chain \$110,000 as a result of a substantial data breach. Know that this is not the credit card companies imposing this fine; this is the state of Massachusetts which is a trend that other states may very well follow in the near future.

There are two key lessons to take away from this second incident. First, it doesn't matter what brand of POS a customer is using, the POS system is not typically the source of the breach. Criminals target insecure networks. This particular chain happened to be using Micros. If you are ever in a situation where a competitor tries to tell a customer that Radiant does not have a secure or "compliant" product; know that there are many examples of incidents involving other POS vendors. ***Criminal attacks in the small business space are POS agnostic and are not unique to or targeted toward Radiant.***

The second lesson is to make sure that you are ***escalating any potential data security breach to Radiant's data security team as soon as possible***. Once notified, merchants only have a short window of time to cooperate with law enforcement or card brand investigations, contain the breach and remediate the site as soon as possible so more cards don't get compromised. One of the main reasons for the large amount of the fine in the Massachusetts incident was that fact that the restaurant chain did not act quickly enough to secure their network and validate their PCI compliance after they were identified as a Common Point of Purchase (CPP).

One of the best risk mitigation activities Radiant and our channel partners can undertake is to continually educate our customers on their responsibilities under PCI. Ignorance of requirements or denial of a problem are not valid defenses against fines or loss of brand reputation.

Use the following links for more information on these above mentioned incidents:

<http://storefrontbacktalk.com/securityfraud/epsilon-breach-may-finally-force-data-handling-rule-changesand-its-only-about-five-years-late/#ixzz1JQXC9W9h>

<http://storefrontbacktalk.com/securityfraud/restaurant-data-breach-probe-filing-card-data-in-plain-text-default-passwords-and-wide-open-wireless-access/#ixzz1JQXJnaTJ>