Questions from 2019 eCommerce Conference

- Is the use of things like Apple Pay and Samsung Pay at a retail location significantly more secure than using a card?
    - In most cases, there is no credit card data presented but just a token. It isn't in scope for PCI since there isn't a Visa, Mastercard, Amex, etc., in use. The payment card data is stored at Apple, Samsung, etc.
- Why does it take so long to discover that a company has been hacked?
    - Because the bad guys want to collect new cards for as long as possible so they don't make themselves known. Once the company knows they have been hacked, there may be internal, external, or FBI investigations to find out what was done and try to catch the bad guys before they let the world know that they were breached. The banks and card brands must be notified in a timely basis since they are the ones financially at risk.
- Does 12.8 and 12.9 speak to liability for fines?
    - 12.8 is all about vendor management. The merchant is liable for everything unless they have identified that a third party is responsible for the requirement. If the vendor has taken responsibility, (12.9) and that is the cause of the breach and/or fines, the vendor is liable.
- When is URL redirect not in PCI scope?
    - When it is being hosted and managed by a PCI compliant third-party vendor. It is still in scope but covered under the AOC (Attestation of Compliance) for that vendor.
- I have a question from the conference that came up regarding our environment. We have a café located on our campus that is contracted by a third party. They have their own internet connection from which they process credit cards. However, this entity contracts space on our campus using our physical ethernet lines to submit the credit card transactions (even though it's not through our internet connection). Since they serve our students from our campus, are we violating any PCI compliance rules by allowing them to work in this manner? Thank you for any insight!
    - If the school isn't providing any services, they wouldn't be considered a service provider to the merchant. It would be a best practice to ask for their AOC every year to ensure they are PCI compliant. It would also be prudent to review the contract for that space to see what the contract says the school is providing and for which it is responsible.
- From the first presentation, P2PE, Security & Mobile Payments, does that mean the FD130 machines with TransArmor are not P2PE?
    - The FD130 is E2E with TransArmor and is not P2PE. Still secure, just not eligible for the P2PE SAQ. Adding TransArmor also reduces PCI scope.
- I do have a couple of questions regarding the CVV codes for credit card transactions. We are trying to find out whether or not PayPal and SunTrust will charge additional fees for using the CVV feature. We've pulled all the paperwork, and it is not completely clear.
    - There is no fee for cvv.