Chip Card Storm Brews

As the October 2020 EMV liability shift at the pump draws near, the cost of NOT taking action grows clear.

By Jeremie Myhren | May 9, 2019

No other industry has as many unattended outdoor payment terminals as we do in the convenience store and petroleum industry in the U.S. There isn't even a close second.

This becomes increasingly relevant to the data security conversation as the payments technology and security landscape continues to evolve. Outdoor payment terminals are steadily increasing in value as a tool used by the criminal underworld.

The October 2015 inside Europay, Mastercard and Visa (EMV) liability shift in the U.S. moved a material percentage of retail payment card transactions from traditional magnetic stripe swipe to inserted, chip-card read. While attackers moved to exploit chip where they could, through techniques like swipe fallback, the retail shift to chip added cost, complexity and reduced feasibility for the criminal hacking groups and gangs who perpetrate most of the large-scale payment-card breaches.

That's not to imply that inside EMV solves the payment card data security problem. In most cases, payment terminals are just as susceptible to a costly compromise as before EMV. Typical breach methods like memory scraping point-of-sale (POS) malware remain a threat, and the data captured in such an attack remains valuable, even from a chipped card. Really, the biggest shift in the move to inside chip is that your outlet becomes less attractive for criminal syndicates to perpetrate the final step of the payment-card data-breach fraud — actually spending the money or using the compromised account to buy goods or services to then sell or trade for cash.

That said, today, few of us have fully operational EMV-capable payment-card terminals at the pump. Many of us have some sites and lanes with chip-capable hardware, but few retailers and payment networks are conducting an actual chip-card read at the fuel island.

The EMV liability shift at the fuel island currently stands at October 2020 and is unlikely to be extended further. Until the liability shift actually takes effect, so long as we follow current acceptance rules (things like not authorizing over allowed limits), we're largely protected from stolen account numbers being used for purchases at our outdoor payment terminals.

This conceals the reality that our c-store sites are seeing higher incidences of stolen or breached payment cards being used for fuel purchases. Thieves are finding more obstacles at their traditional outlets, which have fully converted to chip-card acceptance, so the non-EMV-accepting fuel dispensers have increased in value to them. Because the issuing banks behind the stolen cards being used are bearing the cost of most of this fraud, we are often blind to it — even as it rises steadily.

This sets us up for a troublesome late 2020. Those who do not make the necessary investments in chip-accepting hardware at the fuel island, as well as those who have, but whose POS and payment processing partners have not, will find a shock in November 2020 as they bear the full burden of payment-card fraud at the fuel island for the first time.

What's A Retailer to Do?

- If you are branded, ask your fuel brand what your options are and what the current state of their technology programs are when it comes to EMV at the pump.
- Talk to your POS software and hardware providers to determine dispenser EMV options and when they will be ready.
- Talk to your dispenser partners about your specific dispensers and what your specific options are.
- Talk to your payment-card processors about your specific technology mix and when they will be ready for your specific setup.
- Talk to Visa, Mastercard, American Express and Discover. If you do not have an assigned representative from each payment brand, ask your payment-card processor to put you in touch. Ask each payment brand to share the burden of Automated Fuel Dispenser (AFD) fraud at your sites for the past year. Normally, you do not see this data, as you didn't bear the burden of it, but they have it and are generally able to provide it.
- Use all of the above to apply pressure where needed to get various stakeholders to get you ready in time. Also use it to build your business case and ROI needed to fund the necessary investments to be prepared.