Grocers' Commitment to Customers' Payment Data Security

Consumer Safety

Customer safety is the supermarket industry's top priority. From the safety of the food we sell, to the safety and security of our customers and their payment and shopping data, the grocery industry is committed to protecting our customers. Retailers spend over $6.5 billion each year trying to protect against card fraud.

There is no failsafe technology to protect against breaches for any type of company. Even companies that spend millions on data security and meet and exceed current standards, such as PCI, and protocols for data protection can still find themselves victims of a criminal breach. Unfortunately, this is a fact of the modern marketplace. Food retailers and wholesalers are committed to taking every step possible to prevent breaches, and if they do occur, quickly identifying them and mitigating any damage to customers.

Key Points

1.) Buy-In by All Links in the Payments Chain

Trade associations representing the retail industry, the card networks, issuing banks and processors came together to create a coalition to share information and find ways to strengthen and promote more effective security in the payments system. Today's solutions and future technological improvements will need buy-in by all parties to ensure customer data is protected throughout the payments chain.

2.) Creating More Secure Transactions

The use of personal identification number and chip-enabled credit and debit cards ('PIN and chip') has been successful in Europe and Canada during the shift to EMV payment standards. The PIN and chip technology reduces the risks associated with breaches by making it more difficult to counterfeit cards and/or add unauthorized users. Grocers support the universal implementation in the U.S. payment card system of PIN security along with chip-embedded cards.

PIN authentication shows that the user is the right person. It is much safer than signature; in fact, the Federal Reserve has found that for debit transactions, PIN transactions have one-sixth the amount of fraud losses than signature transactions. Chip cards use an embedded microchip to store and transmit encrypted data.

Advancements in technology beyond PIN and chip are quickly making cards with magnetic strip technology obsolete. Mobile devices offer opportunities to leverage dynamic, tokenized payment data. By employing a one-time token and sophisticated algorithm, the technology would reduce or eliminate the use of actual account numbers or credentials. Mobile also offers additional user verification solutions, such as biometrics or two-factor authentication and user location technology, all of which add additional layers of security. Grocers do not want technology standards to be imposed that would limit future competition in the mobile payments space.

3.) Retailers Already Bear the Significant Cost of a Breach

Contrary to some reports, under both the Visa and MasterCard operating rules, retailers pay for both card reissuance and fraud resulting from a retailer breach. This is a contractual agreement that all retailers have to adhere to in order to accept Visa and MasterCard cards. Any effort to try and legislatively require retailers to pay for additional reissuance would be redundant and unnecessary. Retailers also pre-pay for fraud with swipe fees (1 cent of the swipe fee the Federal Reserve placed on debit cards specifically covers fraud).

4.) Any Legislation Should Hold All Parties to the Same Standard

Criminals target the weakest link in the payments chain. Therefore, the issuing banks, processors and networks should be held to the same standard as retailers.

We support the universal implementation of PIN security along with chip-embedded cards. It makes no sense to spend significant resources to upgrade technology to be able to accept chip cards without additional security features including a PIN. We support technology neutral solutions to ensure competition in the payments space in the future.