SB217/HB117 Maryland Personal Information Protection Act - Revisions
House Ways and Means Committee
Position: OPPOSSE
January 27, 2021

Merchants Work Hard to Protect the Sensitive Information of Their Customers

- Merchants rely on the trust and confidence of their customers and do not want to jeopardize that relationship – especially when it comes to information their customers give them. Merchants are keenly aware that customers have a choice and want to keep them happy, especially in today's most challenging retail environment.

- Merchants share the concern that Marylanders rightly expect their credit card and sensitive personal data will be protected. Merchants are concerned, however, that SB217/HB117 will do little to protect consumers and are in strong opposition to the legislation.

The Credit Card Payment System is Complex
Government Must Take Care When Choosing Sides

- SB 217/HB117 would insert the state into a credit card system governed by a complex series of contractual agreements. Each credit/debit card transaction involves a number of parties – the retailer, the retailer's acquiring bank, the card associations, card processors and the bank that issued the card to the consumer. They interact through a system of complex contractual relationships.

- The credit card system includes a streamlined procedure created by the card associations to deal with data breaches. Generally, they look at card usage and work with issuing banks and companies to investigate possible data breaches. They then report their findings to the financial institutions that issued the impacted cards and the issuing institution then decides whether to monitor, close or block the credit card account. Unfortunately, there is no exact science to tie fraud on an individual credit or debit card account back to a single data breach incident

- The question of who pays what to whom after a breach is governed by the system agreements. Under card association rules, the breached retailer's acquiring bank is liable for the incremental fraud costs during the event window (typically 12- 13 months). The banks that issued the credit cards are entitled to recoup a set amount to cover their costs, including costs to re-issue cards. These banks then collect these charges from the acquiring bank that, in turn, collects them from the merchant.

Some Card Issuers offer their Customers more Protection than Others

- Larger bank issuers protect their customers with sophisticated fraud detection systems. They generally monitor accounts for fraud and close an account (forcing the consumer to use a new card) only if the rate of fraud they are detecting from a known or suspected data breach incident indicates this is a prudent step. Small bank issuers that, much to the disappointment of Merchants, are not required to monitor for fraud under the current system, generally choose to cancel and re-issue all of the cards involved in a breach incident.

- This system, while far from perfect for merchants and banks alike, attempts to balance the equities between all of the parties involved. Any interference by the government in this balance should be measured, as it may skew the cost of security disproportionately to merchants and leave issuing banks little incentive to protect their customers' cards.

SB 217/117 does not Protect Consumers and will Hurt Maryland Employers

- The bill would do little to improve data security but would significantly expand the potential for wasteful, frivolous litigation over security breaches.

- The bill purports to impose state regulation on a complex commercial system that already allocates responsibilities and liabilities. This additional regulation is not necessary and could be counter-productive.

- The bill would pluck a single contract clause (compliance with payment card industry data security standards) out of a complex commercial system and elevate it to the status of state law. This would destroy the balance and integrity of the system. (**Note: Merchants have long advocated that the system would benefit from greater transparency**).

- Payment card industry data security standards are created by the credit card associations. These associations can change the standards at any time they choose – and year over year, they have been modified. Under this bill, whenever these card associations change the standards Maryland state law would change with them, without any opportunity for the Maryland Legislature to protect the public interest. The bill thus would abrogate the power of the Maryland Legislature to make law and hand it instead to the credit card associations.

- Marylanders may be misled by the bill's false promise of consumer protection. The bill would not apply to financial institutions, educational institutions or governmental entities. This despite the fact that 23% of reported privacy breaches involved educational institutions and 31% involved governmental entities. Only 4% involved Merchants.

- The bill would single out one party – Owners of Data - in a complex commercial system and impose unlimited liability regardless of how large or small the business is, whether it was the victim of criminal behavior, or whether it acted negligently.

- The bill would require Maryland merchants to pay money to financial institutions without any check on whether the amounts the institutions claim are reasonable and appropriate. Thus, this legislation would give the financial institutions a blank check drawn on the business' account.

- The bill would require small Maryland businesses to reimburse multi-billion dollar credit unions even when those credit unions make an enormous profit on their credit card operations. This would only encourage credit unions to continue their practice of unnecessary card replacement instead of implementing responsible fraud prevention and detection practices.

- The bill contains numerous undefined terms and potential conflicts with other private sector data security standards. The uncertainty from this language will only increase as private sector standards evolve over time.

- The argument that the bill will encourage merchants to make their systems more secure is a smokescreen. The true purpose of the bill is to benefit the credit unions and small banks. Merchants already face crippling penalties under the card associations' security standards. As an example, TJX paid Visa and the bank that processed TJX's credit payments $40.9 million following the TJX breach disclosed in 2007.

- Bill proponents hold up the TJX breach to taint all merchants while they have been silent about the security failings of many financial institutions. Many small banks choose not to engage in the fraud monitoring that other institutions maintain even though this service is available to them.

- Since small or community banks opt not to "front load" the security of their cards through neural networks and other monitoring systems, they gamble with the cost of reissuing cards every day.

Now they are asking the Legislature to help them push those costs and more back on the merchants and other owners of data. We are asking you to vote unfavorably on HB117.