Comment: Scathing attack on Visa and MasterCard for their "broken payments system"
Target breach highlights lack of investment in card security says MPC counsel

Doug Kantor, legal counsel for the Merchant Payments Council has made a scathing attack on Visa and MasterCard, for making a collective US$1.8bn profit from a "broken payments system" and for making merchants pay for security breaches such as the monumental one just suffered by retailer Target.

Kantor argues that Visa and MasterCard, "while controlling all of the elements related to the operation of their card networks – including the swipe fees, the largest part of what merchants are charged to accept the cards, how consumers' account information is protected and who pays for fraud" have minimal exposure to any financial loss related to security flaws in their product.

He writes in The American Banker: "While Visa and MasterCard dictate card security and allow transactions to proceed without authentication or encryption, they have little real interest in implementing effective security because they don't absorb many fraud losses."

He also refutes claims that the Durbin Amendment to the Dodd-Frank Act has caused the problem. It is argued that the reduced card fees required by the Durbin Amendment, have led to less being spent on security. Kantor says no. " Under Durbin, merchants paid $250 million in special interchange fees over the past year to the largest banks covered by the Durbin amendment to "innovate" data security methods that better protect the consumer. Any contention that Durbin may have financially hamstrung issuing banks (the fewer than 200 covered under Durbin) from doing the right thing is just wrong."

Merchants have invested tens of billions of dollars over the past five years in securing the estimated 12.6 million "endpoints" where consumers transact as part of the card brands' mandates for improved data security. But much of that money was spent just to comply with Payment Card Industry security standards. PCI is controlled by the major card companies and, instead of focusing on the most effective anti-fraud systems possible, such as simply requiring the use of PIN, PCI focuses on pushing costs onto merchants. Target was in compliance with PCI standards. Clearly that wasn't enough."

Kantor says the associations have not taken on "real card security" in the US and to a point he

is right. The US is years behind most of the rest of the world, because the country's collective payments industry, and this includes the merchants as a major party, has refused to invest in new technology, until now. It was always argued that the 100% online authentication of payments made the US a safe place for card transactions. With the US now the leading fraud destination for fraudsters, this is very definitely no longer the case.

And then there is the thorny issue of PCI. The card associations and the PCI Security Standards Council have always been adamant on two counts. The first is that if a merchant is PCI compliant, a card data breach is not possible. The second is that payments security is a moving and evolving goal. Fraud threats change all the time, and importantly, so does the merchant environment. It only takes an IT person to change a setting, or for an employee to pull out a plug and a data centre can go from compliance to high risk in an instant. The fact that a merchant or a data centre was compliant at their last inspection is not relevant.

It is a fundamental PCI rule that card data should not be stored. Period. For Target to be a victim, it must have broken this rule, although it claims it is only encrypted PINs that have been stolen. We have yet to learn exactly how this breach happened, or the extent of the fall-out, but experience so far has shown that it is always a lack of adherence to the PCI rules that causes a breach in the first place. This may not be by the merchant, it could be through a third party, as in the TJX/TK Maxx breach.

PCI standards are constantly being honed to keep payments secure. This takes investment and diligence. Who should pay for it is another matter.

Card World has asked MasterCard Worldwide and Visa Inc for comment and is awaiting a response.