Response from EMVCo to the Cambridge University Report on Chip and PIN vulnerabilities ('*Chip and PIN is Broken*' - February 2010):

The EMV Specifications for payment cards and terminals provide interoperability and security features, which act as building blocks for the payment systems and financial institutions to design their products and processes according to their wider risk management needs. It is EMVCo's view that when the full payment process is taken into account, suitable countermeasures to the attack described in the recent Cambridge Report are already available.

The scenario described in the report requires the presence of a stolen card and in addition does not apply to ATM transactions. The possible financial impact is therefore limited while the risk of exposure of the fraudster is significant.

Countermeasures and controls including authorisation data checks, fraud modeling and other forensic processes are available within EMV functionality, payment system products and networks, and issuer host systems. These are sufficient for resolving cardholder disputes.

As the EMV Specification is one piece of the overall payment transaction as managed by payment systems, EMVCo refers further media queries on this subject to the individual payment systems who can respond to questions in the context of their full fraud management controls.