



Response from EMVCo to the Inverse Path Paper 'Chip and PIN is Definitely Broken – March 2011'

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 and acceptance requirements. In response to the report in March 2011 'Chip and PIN is Definitely Broken', it is EMVCo's view that when the full payment process is taken into account, suitable countermeasures are available.

For example, it is well known that PINs can be stolen by the use of a variety of techniques (e.g. PIN pad overlays, hidden cameras, shoulder surfing, bogus terminals, social engineering). Using a rogue shim in a terminal supporting offline plaintext PIN (possibly subverting the card's PIN encipherment preferences and causing an offline card authentication failure or even a decline) is another technique. The mitigation against this threat is that no transaction can be performed without also stealing the card where card cryptography operations are required for a successful transaction. This allows normal lost and stolen payment system protections to apply. Conversely the mitigation against a genuine card being abused if lost or stolen is that the thief will not have access to the PIN, hence the PIN has a role to play despite the 'eavesdropping threat' and remains an important tool for protecting against lost and stolen fraud.