Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, December 2012, vol. 17, no.3
(http://www.arraydev.com/commerce/jibc/)

Calling for a Uniform Approach to Card Fraud Offline and On

STEPHEN WILSON
Managing Director, Lockstep Technologies, Sydney, Australia
Postal Address: **11 Minnesota Ave, Five Dock (Sydney) NSW 2046, Australia**
Author's Personal/Organizational Website: **http://lockstep.com.au/technologies**
Email: **swilson@lockstep.com.au**
Stephen Wilson, Principal of Lockstep Consulting (Sydney, Australia) is an information security researcher and analyst, with a special interest in smart technologies and PKI for protecting digital identity and privacy.

Abstract

The credit card payments system is a paragon of standardisation. No other industry has such a strong history of driving and adopting uniform technologies, infrastructure and business processes. No matter where you keep a bank account, you can use a globally branded credit card to go shopping in almost every corner of the world. The universal Four Party settlement model, and a long-standing card standard that works the same with ATMs and merchant terminals everywhere underpin seamless convenience. So with this determination to facilitate trustworthy and supremely convenient spending in every corner of the earth, it's astonishing that the industry is still yet to standardise Internet payments. We settled on the EMV standard for in-store transactions, but online we use a wide range of confusing and largely ineffective security measures. As a result, Card Not Present (CNP) fraud is growing unchecked. This article argues that all card payments should be properly secured using standardised hardware. In particular, CNP transactions should use the very same EMV chip and cryptography as do card present payments.

Keywords: **cards; payments; fraud; CNP fraud; security; EMV; chip and PIN; Australia**

INTRODUCTION

The latest bi-annual card fraud statistics released by the Australian Payments Clearing Association are startling (APCA, 2012a). Card Not Present (CNP) fraud now represents three quarters of all card fraud in Australia and is growing unchecked at over 50% per annum. Lockstep Consulting monitors the APCA releases and compiles a longitudinal series. The latest Australian card fraud figures are summarised below.

Figure 1

Trends in Australian Credit Card Fraud Categories CY 2006-11

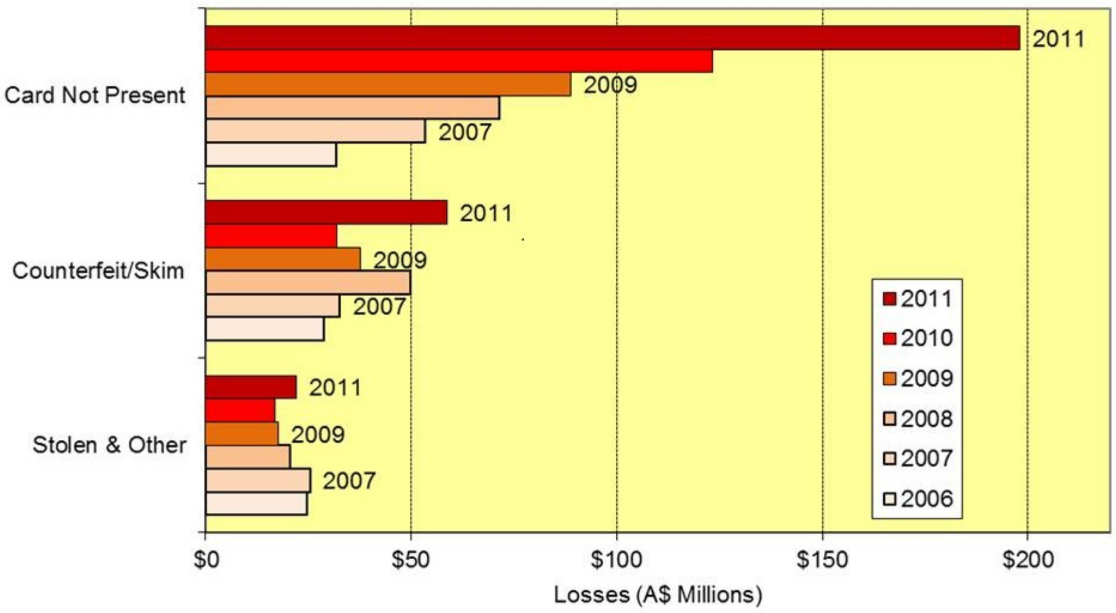

Diagram Copyright © Lockstep Consulting 2012

APCA's only comment in its latest press release on the CNP crime wave is to associate it with the popularity of e-commerce. "[The increase in CNP fraud] broadly reflects growing retail activity in the online space, with many more businesses, in particular small and medium sized retailers, moving online. For those new to the online space, it can take time to implement safe and effective practices to protect against CNP fraud" (APCA, 2012b). That's a bit like the automotive industry putting up with a high road toll because people love driving.

Until now, APCA promoted the credit card scheme's *3D Secure* protocol as a response to CNP fraud. APCA's previous three bi-annual card fraud press releases all mentioned the work by MasterCard and Visa on 3D Secure (APCA, 2010, 2011a, 2012b); in June 2011 the APCA CEO went so far as to say "retailers should be looking at a 3D Secure solution for their online checkout" (2011a). But APCA's most recent press release makes no mention of 3D Secure at all. I speculate that 3D Secure, after many years of disappointing performance and take-up, is now too contentious to be promoted by Australia's regulators.

If 3D Secure doesn't rate a mention anymore, where does that leave merchants and cardholders wanting to shop online? Frankly it's a mystery why the payments industry seems so bamboozled by CNP fraud, because technically it's a very simple problem. And it's one we've already solved elsewhere. Card Not Present fraud is simply online carding.

SKIMMING AND CARDING

In carding, criminals replicate stolen customer data on blank cards; with CNP fraud they replay stolen data on merchant servers.

A magstripe card stores the customer's details as a string of ones and zeroes, and presents them to a POS terminal or ATM in the clear. It's child's play for criminals to scan the bits and copy them to a blank card.

The industry responded to skimming and carding with EMV (aka Chip-and-PIN). EMV replaces the magnetic storage with an integrated circuit, but more importantly, it secures the data transmitted from card to terminal. EMV works by first digitally signing those ones and zeros in the chip, and then verifying the signature at the terminal. The signing uses a Private Key unique to the cardholder and held safely inside the chip where it cannot be tampered with by fraudsters. It is not feasible to replicate the digital signature without having access to the inner workings of the chip, and thus EMV cards resist carding.

ONLINE CARD FRAUD

Conventional Card Not Present (CNP) transactions are vulnerable because, like the old magstripe cards, they rest on cleartext cardholder data. On its own, a merchant server cannot tell the difference between the original card data and a copy, just as a terminal cannot tell an original magstripe card from a criminal's copy.

Despite the simplicity of the root problem, the past decade has seen a bewildering patchwork of flimsy and expensive online payments fixes. Various One Time Passwords have come and gone, from scratchy cards to electronic key fobs. Temporary SMS codes have been popular but were recently declared unsafe by the Communications Alliance in Australia, a policy body representing the major mobile carriers.

Meanwhile, extraordinary resources have been squandered on the novel “3D Secure” scheme (MasterCard SecureCode and Verified by Visa). 3D Secure take-up is piecemeal; it's widely derided by merchants and customers alike. It upsets the underlying Four Party settlements architecture, slowing transactions to a crawl and introducing untold legal complexities.

So why doesn't the card payments industry go back to its roots, preserve its global architecture and standards, and tackle the real issue? We could stop most online fraud by using the same chip technologies we deployed to kill off skimming.

It is technically simple to reproduce the familiar card-present user experience in a standard computer. It would just take the will of the financial services industry to make payments by smartcard standard. There are plenty of smartcard reader solutions on the market and indeed, many notebooks feature built-in readers. Demand for readers has grown steadily over the years, driven by the increasing normal use of smartcards for e-health and online voting in Eastern Europe and Asia.

With dual interface and contactless smartcards, the interface options open right up. NFC devices like most tablets and smartphones can switch into Card Reader Emulation mode, to act as a smartcard terminal. Alternatively, the SIM or Secure Element of most mobile devices could be used to digitally sign card transactions directly.

CONCLUSION

All serious payments systems use hardware security. The classic examples include SIM cards, EMV, the Hardware Security Modules mandated by regulators in all ATMs, and the Secure Elements of NFC devices. With well-designed hardware security, we gain a lasting upper hand in the cybercrime arms race.

The Internet and mobile channels will one day overtake the traditional physical payments medium. Indeed, commentators already like to say that the “digital economy” is simply the economy. Therefore, let us stop struggling with stopgap Internet security measures, and let us stop pretending that PCI-DSS audits will stop organised crime stealing card numbers by the million. Instead, we should kill two birds with one stone, and use chip technology to secure both card present and CNP transactions, to deliver the same high standards of usability and security in all channels.

REFERENCES

APCA Australian Payments Clearing Association (2012a). Payment Fraud Statistics - Fraud Perpetrated on Australian Issued Payment Instruments, 1 January 2011 - 31 December 2011 http://www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-calendar-year-2011.pdf

APCA Australian Payments Clearing Association (2012b). Media Release: Payments fraud in Australia 12 July 2012 http://www.apca.com.au/docs/2012-media-releases/payments-fraud-statistics-for-calendar-year-2011.pdf

APCA Australian Payments Clearing Association (2011a). Media Release: Payments fraud in Australia 15 December 2011 http://www.apca.com.au/docs/2011-media-releases/payments-fraud-statistics-for-financial-year-2011.pdf

APCA Australian Payments Clearing Association (2011b). Media Release: Payments fraud in Australia 22 June 2011 http://www.apca.com.au/docs/2011-media-releases/payments-fraud-statistics-for-calendar-year-2010.pdf

APCA Australian Payments Clearing Association (2010). Media Release: Payments fraud in Australia 7 December 2010 http://www.apca.com.au/docs/2010-media-releases/payment-fraud-statistics-for-financial-year-2010.pdf