Cardless criminals

Card-not-present fraud is spiraling out of control, with very few options for stopping it

BY STEPHEN WILSON

Card-Not-Present (CNP) fraud is ballooning; it now represents the most prevalent form of credit card crime. APCA in Australia and APACS in the UK recently reported uncannily similar statistics. CNP fraud in both countries now makes up around a half of all payment card fraud, and has grown by around 40 per cent in the last 12 months. What's worse, there is nothing in mainstream security that can actually prevent it.

In this column, I'll explore the fundamentals of the problem – including the industrialisation of identity theft – and describe some groundbreaking research and development that has the promise of stemming CNP fraud for good.

Organised cybercrime is powered by stolen identity data. There is a huge black market in stolen IDs, which are traded in fantastic volumes on clandestine "carding" sites, to criminals that either transfer the data to counterfeit plastic, or simply replay the numbers online to defraud CNP merchants.

The supply and demand for stolen identities are both booming. In Australia, CNP fraud in FY2007 cost $39M or approximately $3.00 p.a. per card. In the UK, the per capita figure is worse, with CNP fraud in 2007 totalling £290M. So it's big business.

On the supply side, we know where cybercriminals are getting their ID data. Major breaches of personal information are now literally a weekly occurrence. A raft of new US laws mandate the reporting of privacy breaches; several public interest websites publish statistics. Attrition.org for instance shows 70 incidents in the US alone for the first 12 weeks of 2008, with something over 4.8 million credit cards compromised.

With stolen credit card numbers so widely available, perpetrating CNP fraud is child's play. And it's becoming all the more appealing to cybercriminals as Internet banking security – including two-factor authentication – has made it difficult to 'hack' directly into customer accounts. Two-factor security mechanisms are not easily extended from a closed online banking situation to the millions of merchants who are accepting credit cards online.

The basic problem is that absolutely nothing stops stolen credit card numbers being replayed online against merchants accepting CNP transactions.

Most strategies to deal with CNP fraud focus on merchants gathering what is purely circumstantial evidence to try and establish the legitimacy of the person sending orders over the Internet. The best advice from card schemes and regulators today[1] is that merchants must ask their customers to provide such personal details as contact phone number, the cardholder's statement address and even the credit card verification number ("CVC" or "CVV" depending on the scheme).

Frankly it's become a bit surreal. CVC/CVV numbers were introduced to combat "dumpster diving". They are not embossed, so they didn't appear on the old carbon paper waste that classically was collected by crooks from the trash behind restaurants and shops. But to now gather CVC/CVV numbers online, alongside the primary account number, is quite simply counter-productive, since it exposes the codes to the very same type of theft that we're trying to protect ourselves from! It's like trying to put out a fire with gasoline.

Online merchants now find themselves collecting vast amounts of personal information which is otherwise irrelevant to their transactions and their customer relationships. This collection intrudes on card holder privacy, is a significant time waster, and adds to the compliance burden of merchants who must take special care to safeguard the data. But worst of all, it's simply futile. As more personal data is collected, the exposure to ID theft is only exacerbated, merchants suffer more attacks and leaks, and the information becomes less and less effective as a weapon against CNP fraud.

Spare a thought too for merchants' ever increasing compliance burden under Payment Card Industry (PCI) security standards. So much of the PCI standards focus on protecting data that wouldn't need to be gathered at all if the credit cards were more trustworthy online.

A possible solution

The main technological thrust in combating online credit card fraud has been around the new payments protocol "3-D Secure" (marketed variously as Verified by Visa and MasterCard SecureCode). It's early days for 3-D Secure, and it will have to prove itself in respect of several critical success factors, including the cost of implementation for merchants, and the cardholder experience.

Lockstep's research has identified an alternate approach to the problem of CNP fraud. We contend the fundamental problem underlying all ID theft is that our personal data loses its pedigree when presented online. Consider credit card numbers: when presented in person, a number is substantiated not only by the cardholder's signature but also by the card itself. Thanks to holograms and other security features, the merchant has a good chance of spotting a fake card.

But when we shift to the online world, the credit card number loses its pedigree. All numbers look the same; e-merchants have no way to tell a stolen number from the real thing.

Lockstep has developed a new way to present credit card numbers online, leveraging EMV cards. By simply taking proper care to safeguard credit card numbers and enable merchants to verify that numbers presented online are genuine, we can restore full confidence in CNP transactions.

Smartcards are now well known in the POS setting; it is high time we turned to them as the best available weapon against CNP fraud and ID theft in general.

1. See for example APACS' Fraud prevention guidelines for CNP retailers at www.netpayments.co.uk/downloads/cnp_booklet.pdf

Stephen Wilson is a leading international authority on identity management and information security. In early 2004, Stephen established Lockstep Consulting to provide independent security advice and to develop new smartcard solutions to identity theft.

swilson@lockstep.com.au