# How to stop Card-Not-Present fraud over the Internet

Card-not-present (CNP) fraud is now the most prevalent form of payment fraud. The risk is mushrooming as consumers have become more comfortable using their cards online and in the process, divulging more and more personal details which are being turned against them by cyber criminals.

CNP fraud amounted to $40 million in Australia in 2007 and is up 46% on the previous year. Overseas the problem is even worse. The raw materials for CNP fraud—credit card details including CCV numbers and personal data—are being stolen on a massive scale, and traded on international cyber crime bulletin boards.

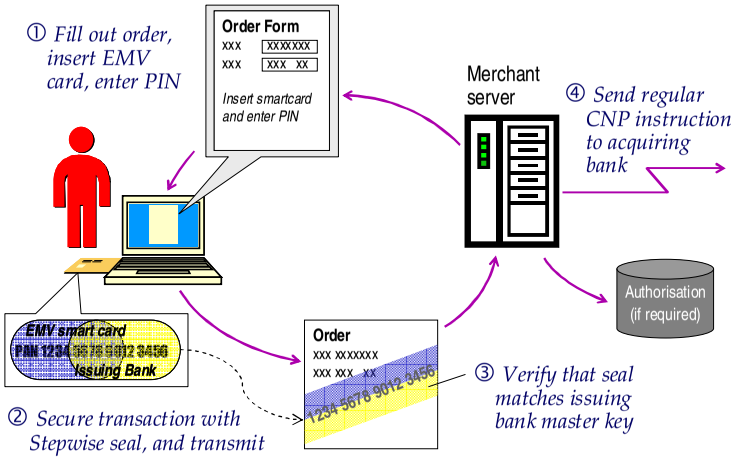
Current strategies to deal with CNP fraud require merchants to ask for increasing amounts of personal detail to try and establish ownership of a credit card. This information is often irrelevant to the transaction, invades cardholder privacy, wastes everyone's time, and adds to the compliance burden and risk for merchants who must then safeguard all this personal data. Perhaps worst of all, these countermeasures only exacerbate the problem. The more personal data that is collected, the more ends up being stolen and exploited by cyber criminals. Gathering more cardholder details to curtail CNP fraud is like trying to put out a fire with gasoline.

## The Lockstep solution

Lockstep Technologies' four year R&D program has resulted in an innovative, economical and uniquely effective weapon against CNP fraud.

Our product *Stepwise* is a specially formatted digital certificate that, when loaded onto an EMV smart credit card, turns it into the best available defence against CNP fraud and ID theft in general.

The diagram illustrates a *Stepwise* CNP transaction.




*Stepwise* encapsulates each cardholder's personal details and credit card number in a tamper proof digital seal. The seal is carried within an EMV chip and applied to each credit card transaction to prove the card details are genuine. The *Stepwise* seal can be processed by any e-commerce server to validate the card details; the seal cannot be replicated unless the bona fide smartcard is present and the PIN entered.

✓ ***Stepwise* requires no change to the interface between merchant and bank.**

✓ ***Stepwise* requires no special card scheme authentication server.**

**The *Stepwise* seal tells the merchant everything they need to know to be sure that a web commerce transaction is valid.** It proves that a bona fide credit card was present, and that the credit card details cannot have been replayed by an impostor or simply made up.

## Benefits of *Stepwise*

### *For cardholders*

- better protects their privacy, with less disclosure of extraneous personal details in routine e-commerce
- simple, fast, EFTPOS-like online shopping experience
- cuts exposure to ID theft arising from compromise of merchant servers or payments processors.

### *For merchants*

- removes the risk of CNP fraud over the Internet
- simple, low cost implementation; no change to the existing interface with acquiring banks; *Stepwise* processing occurs in standard merchant server software
- only collect information actually needed for the business; reduced exposure to attackers seeking to steal customer financial data
- better compliance with Payment Card Industry (PCI) security obligations and privacy legislation.

### *For financial institutions*

- reduced losses from CNP fraud
- improved ROI on EMV cards
- lower cost implementation compared to any other online payment scheme (since no authentication server is required).

Copyright © 2008 Lockstep Technologies Pty Ltd



***"Safety in Numbers"***

www.lockstep.com.au/technologies