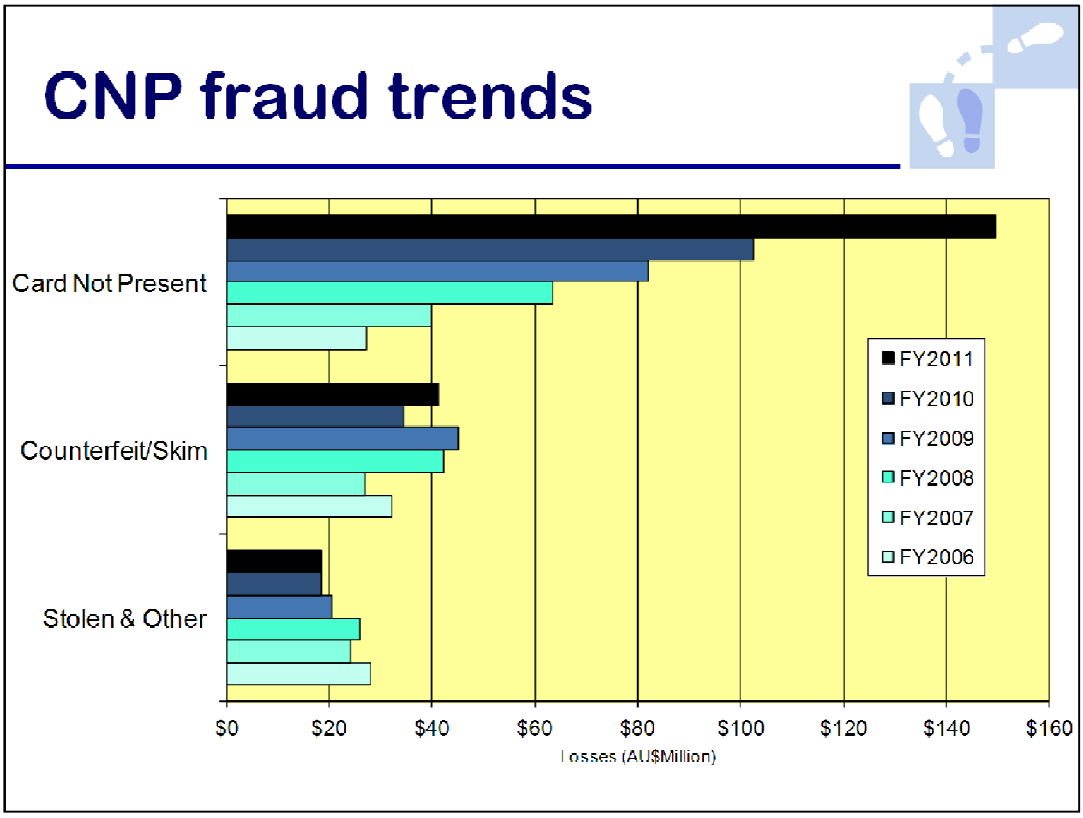
Many thanks to G&D – David Curtis and Australia MD Uli Klink -- for the opportunity to present today some of Lockstep Technologies' secure online payments R&D.

The Lockstep Group comprises two companies. Lockstep Consulting provides research, analysis & advice in digital identity & privacy. Lockstep Technologies develops innovative solutions to identity theft using smart technologies. Today I'll show you how we can solve Card Not Present fraud online, and how Lockstep's core solution may be integrated with the card industry's preferred CNP protocol, "3D Secure".



Every six months the Australian Payment Clearing Association APCA releases card fraud figures for the preceding 12 months. Lockstep monitors these figures and plots the trends on our blog site. Here are the latest figures from late 2011, going back six years.

Card Not Present fraud now accounts for nearly three quarters of all card fraud in Australia. It is rising at around 40% per annum, while card present forms of fraud hold steady thanks mainly to the rollout of chip.

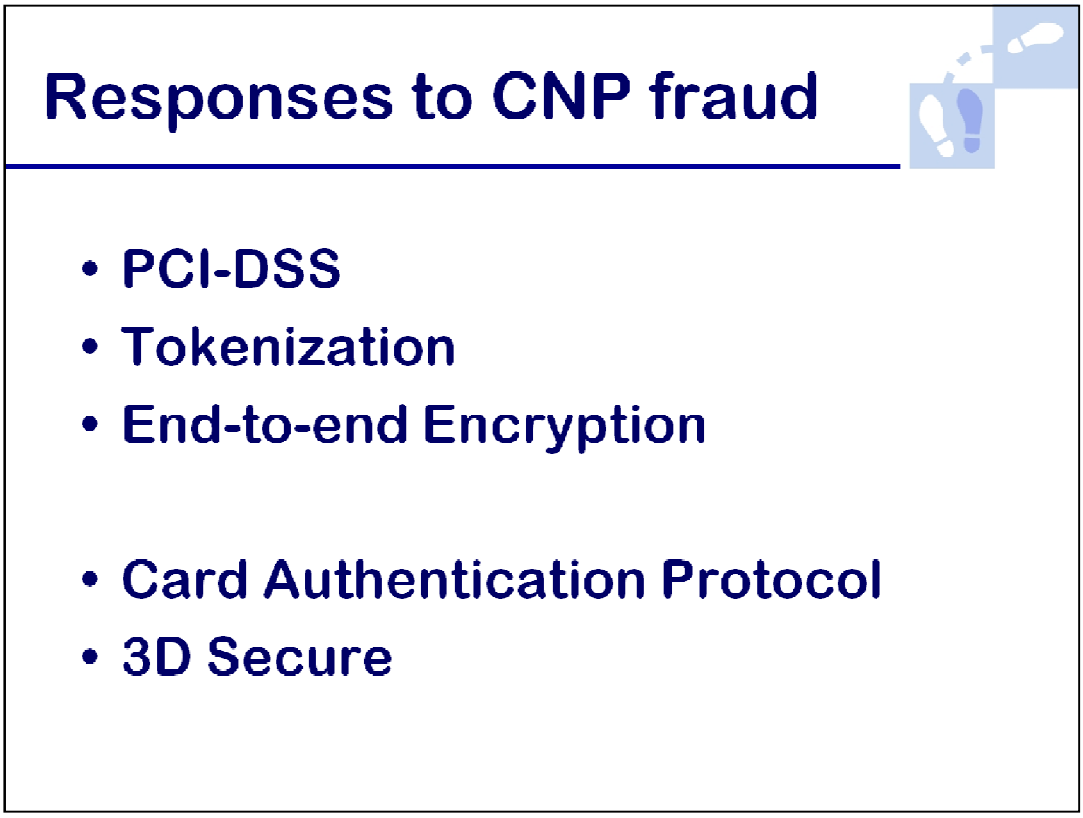
See http://lockstep.com.au/blog/payments.

http://datalossdb.org

Largest Incidents

RECORDS	DATE	ORGANIZATIONS
130,000,000	2009-01-20	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
94,000,000	2007-01-17	TJX Companies Inc.
90,000,000	1984-06-01	TRW, Sears Roebuck
77,000,000	2011-04-26	Sony Corporation
40,000,000	2005-06-19	CardSystems, Visa, MasterCard, American Express
40,000,000	2011-12-26	Tianya
35,000,000	2011-07-28	SK Communications, Nate, Cyworld
35,000,000	2011-11-10	Steam (Valve, Inc.)
32,000,000	2009-12-14	RockYou Inc.
26,500,000	2006-05-22	U.S. Department of Veterans Affairs

CNP fraud is fuelled by card data stolen in bulk by organised cyber crime gangs. This website reports data breaches; here are the worst reported breaches of all time. I've circled cases involving payment card data.



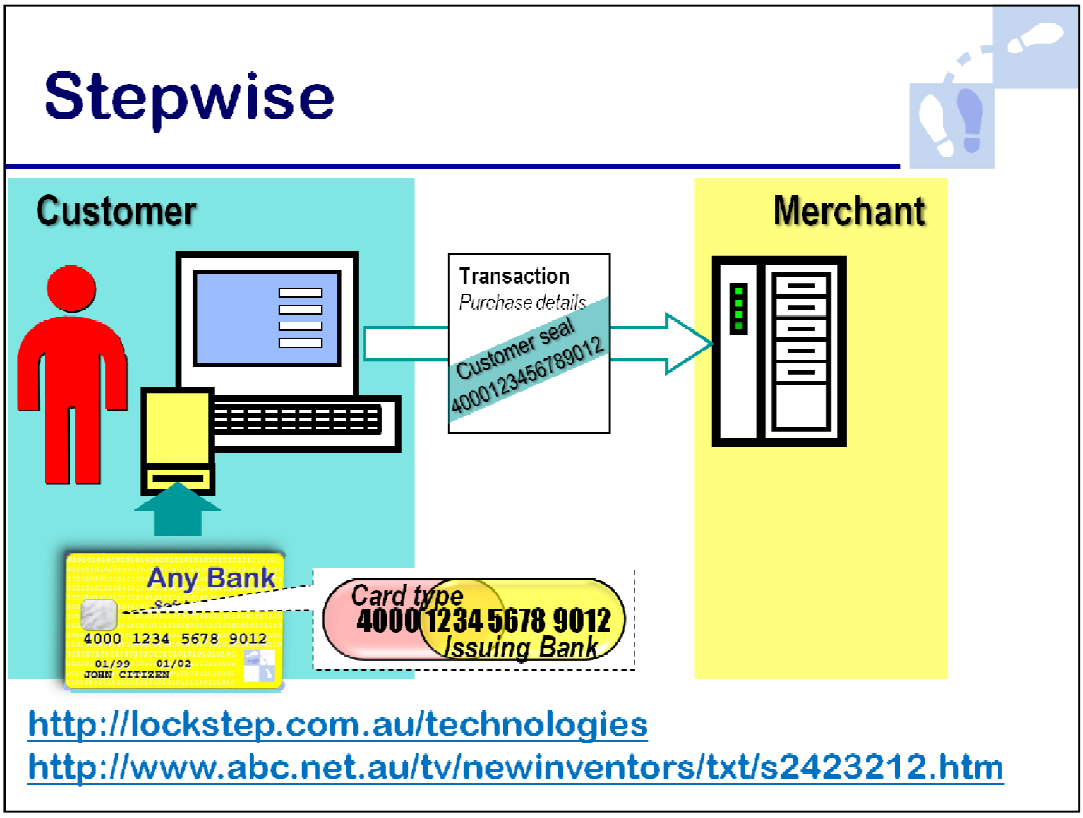
The industry has responded to the CNP fraud problem in a few different ways.

There are attempts to curtail card data theft or to neutralise its effects. The PCI-DSS regime tries to improve security, but frankly it has proven ineffective. It's a security policy and audit based approach. As such, it's good for reducing accidental losses and it repels amateur attacks, but it's powerless against organised crime, Advanced Persistent Threats and corrupt insiders. Referring to the previous slide, the biggest breach of all time involved an organisation that insisted it was PCI compliant. Arguments raged about the true state of Heartland Payments System's PCI audits; the debate even turned to what a PCI audit means. It is outrageous in my opinion that there should be any room for doubt! In the three years since the Heartland breach, it seems people have become bored with PCI-DSS, for when the Sony Play Station Network was breached, the question of PCI compliance didn't even come up.

Tokenization and End-to-End Encryption are major infrastructure programs that seek to reduce the exposure of credit card numbers in organisations handling them. These are expensive solutions that don't in fact prevent anyone abusing credit card numbers once they have obtained them.

On the preventative side, CAP is popular in Europe. It uses the cryptography in an EMV card to generate tamper resistant one time passcodes using a calculator-like stand alone card reader.

Finally we have 3D Secure, a technically sophisticated online payments protocol, developed and promoted by Visa and MasterCard. 3D Secure has turned out to be problematic for many reasons. A particular problem is that it is very slow for users, thanks to a number of protocol bottlenecks. This presentation will show how Lockstep Technologies can reduce those problems and improve take-up.



There is another way to stop CNP fraud: Lockstep Technologies' "Stepwise".

We developed Stepwise as a variant on Lockstep's patented identity theft and anonymisation solution.

A live demo is available at the ABC TV "New Inventors" website, and more technical information at our website (URLs above).

Briefly, in a stand-alone mode, Stepwise is used to "encapsulate" card details in a digital certificate issued to an EMV card, and to then "seal" those details onto each CNP transaction using built-in cryptographic library modules in browsers and servers. Stepwise proves to the merchant server that each CNP payment originated from a genuine credit card, under the control of the cardholder.

Stepwise was developed with the assistance of an Australian Government COMET Grant and the Australian Technology Showcase. It was awarded third place in the Asia Sesames Awards 2010, and was featured in the UK's Finextra Innovation Showcase.

Stepwise can be deployed in a stand-alone mode as illustrated above and in the New Inventors video clip. But this presentation is about how to integrate Stepwise with the card companies' preferred protocol.

Stepwise can be understood as the virtual equivalent of chip based anti-skimming measures. Card Not Present fraud is simply "online skimming".

A magnetic stripe card holds a string of ones and zeros, representing the cardholder details, in the clear, and presents that string to a POS terminal or ATM. Because the ones and zeros appear in the mag stripe in the clear, it's easy for a criminal to scan them and copy them to a blank card. In general terms, EMV or chip-and-PIN works by encrypting the ones and zeros in the chip so they can only be correctly decoded by the terminal equipment. In reality the explanation is somewhat more complex, involving asymmetric cryptography, but for the purposes of explaining the parallel between Stepwise and EMV, we can skip the details. The salient point is that the encryption takes place in the chip using keys that cannot be tampered with or substituted by an attacker.

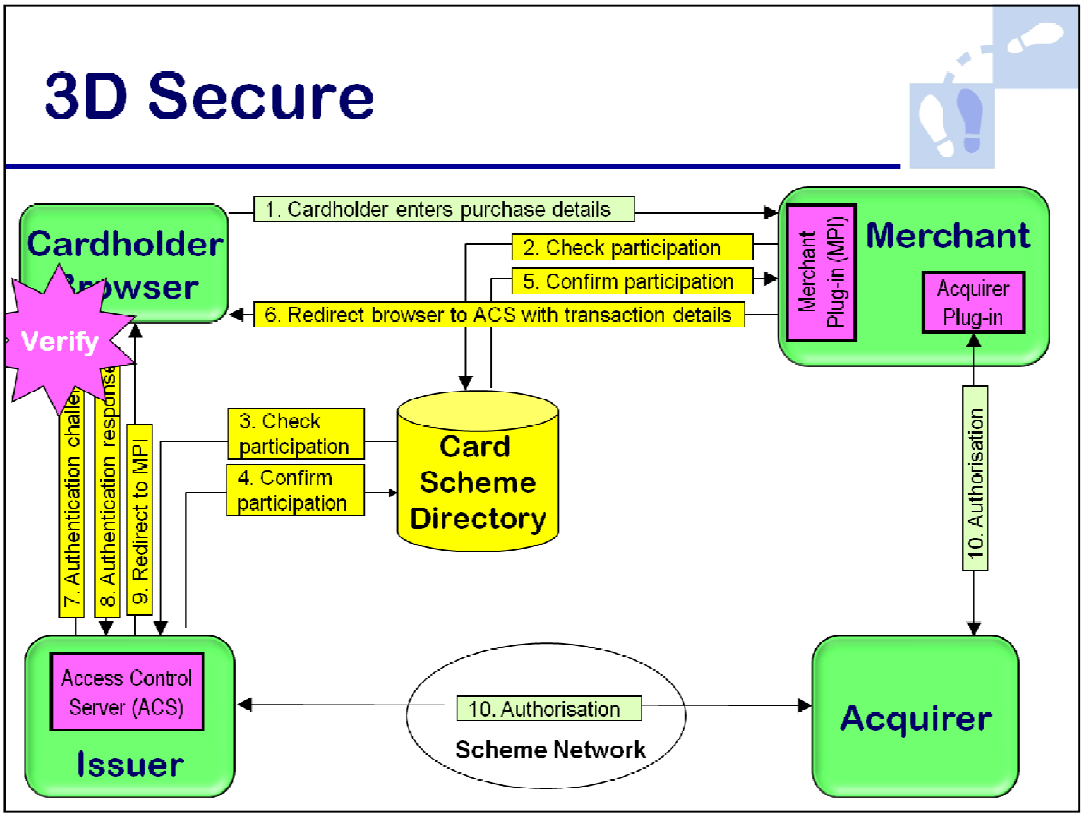
As with mag stripes, conventional Card Not Present transactions involve transmitting cleartext cardholder data, this time to a merchant server. On its own, a server cannot tell the difference between the original data and a copy, leaving merchants vulnerable to CNP fraud using stolen card numbers.

Stepwise is analogous to the use of EMV to prevent skimming. Stepwise uses the standard cryptographic functionality of the chip to uniquely encrypt the cardholder details, in such a away that they can be decrypted at any merchant server, using standard built-in software libraries and a widely distributed Stepwise "master key".

Stepwise is protected by the following patents:

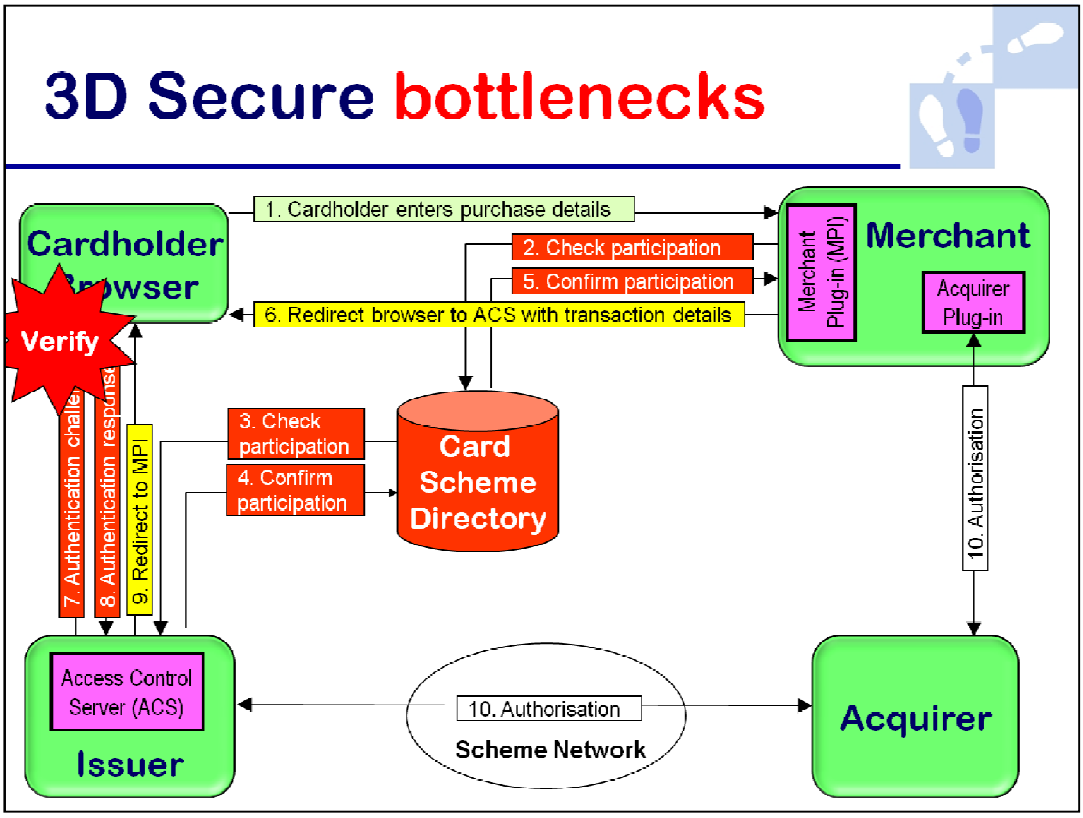
System and method for anonymously indexing electronic record systems; Patent No. PCT/AU2005/000364 (2004)

Authenticating electronic financial transactions; Patent Application PCT/AU2009/000456.



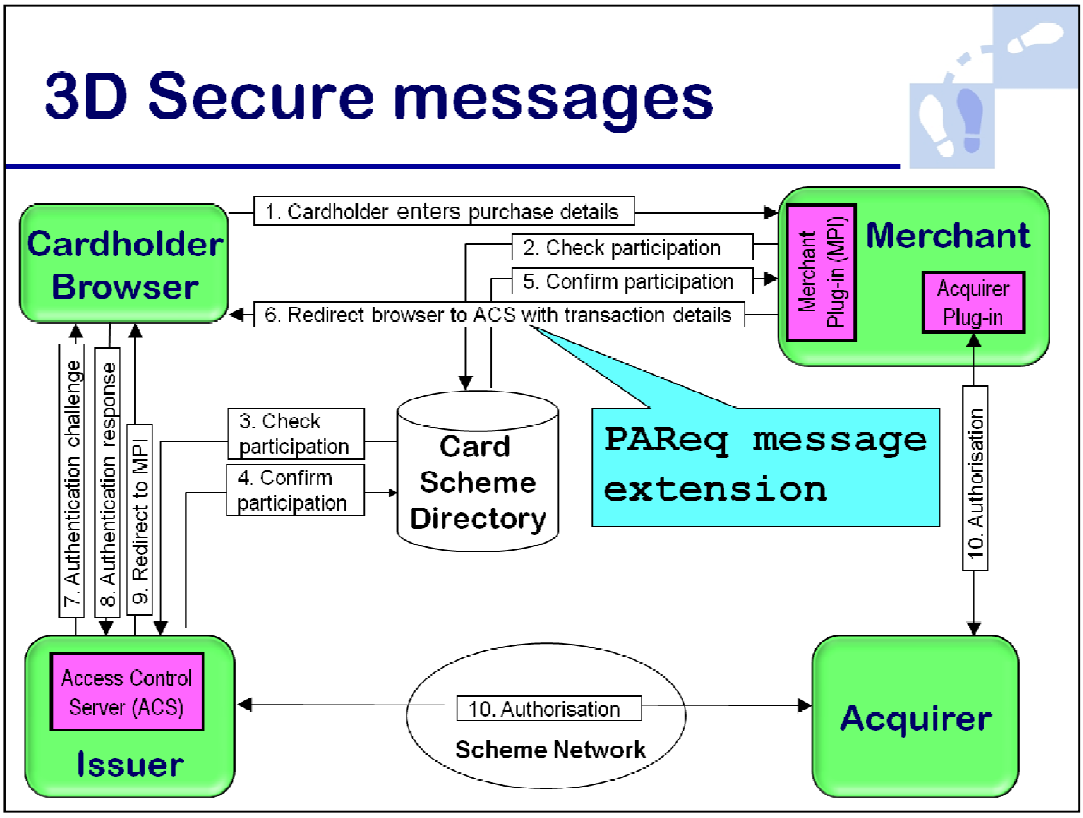
Let's review 3D Secure.

The protocol adds a number of new software sub-systems and components to the customary four corner payments settlement model, and a large number of new steps. Instead of pushing card details from cardholder to merchant and thence to the Acquiring and Issuing banks, 3D Secure involves a series of real-time double checks to attempt to verify the cardholder integrity. After the cardholder initiates the purchase (1), the Merchant server checks with a new scheme directory that the cardholder is in fact enrolled for 3D Secure (2,3,4,5). Then the Merchant server re-directs the customer's browser to the Issuing Bank, a step that undermines the separation of banks in the four party model and is probably unprecedented in card processing. The Issuer then verifies the cardholder identity by some means (7,8) which vary from bank to bank, but usually includes a pop-up dialog box. On successful verification, control reverts to the Merchant server (9) and finally the transaction is sent through to the Acquirer to be completed in the normal manner (10).

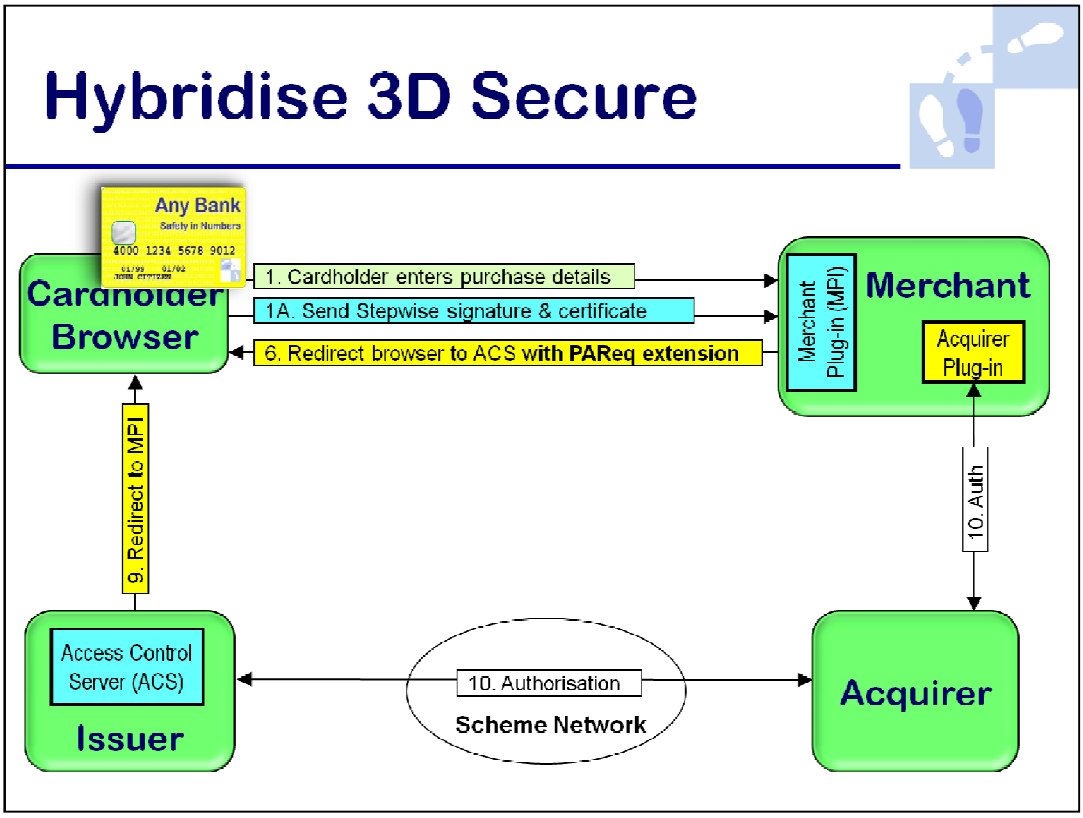


In red are the steps that throttle 3D Secure and the user experience. In particular, the cardholder verification is unusual and disconcerting. Many cardholders see the pop-up dialogue as a phishing attack and ignore it, cancelling the transaction. Indeed, many browsers are set to disable pop-ups and 3D Secure simply fails to establish a connection in those cases.

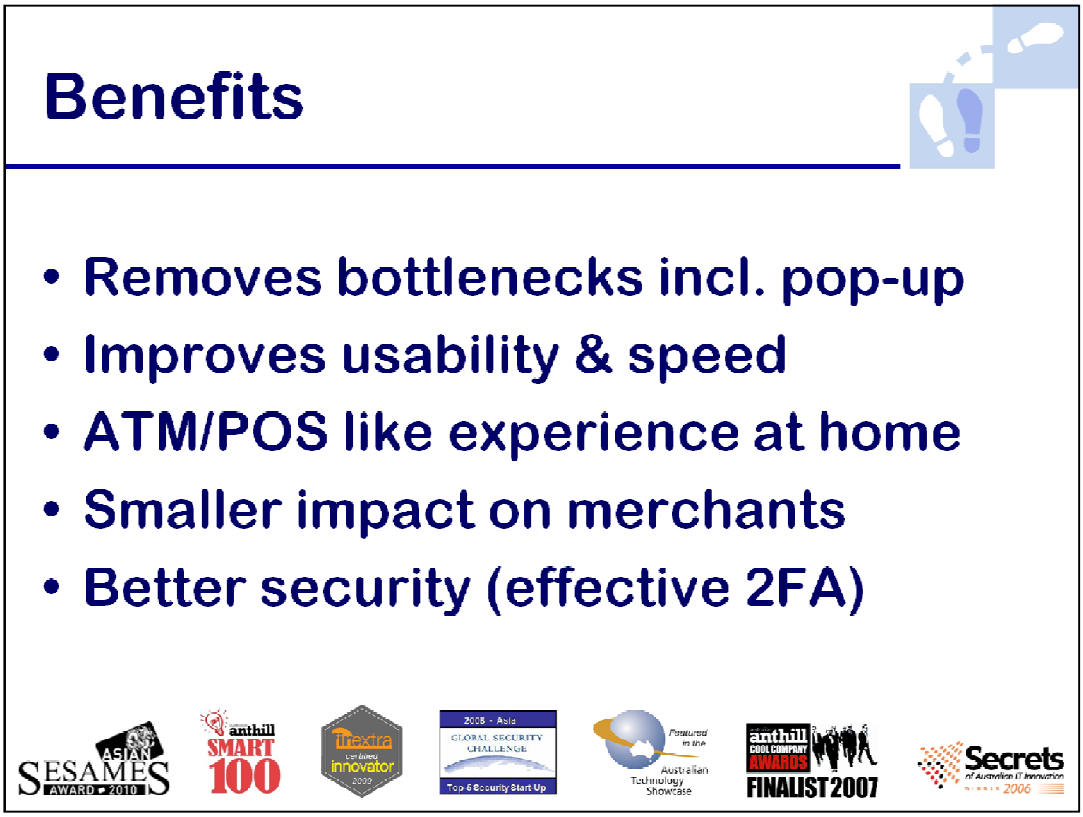
The card schemes themselves have reported 10-15% increase in shopping cart abandonment rates when 3D Secure is introduced. Merchant groups in Europe have estimated that the figure is 40%.



Lockstep Technologies' investigations into 3D Secure found that there is a way to switch off the biggest bottleneck. The protocol includes a message sent from the Merchant to the Issuer called "Payer Authentication Request" (PAReq). A flag can be set in the PAReq message that tells the Issuer they need not perform the cardholder verification. If the browser presents the merchant with evidence that a Stepwise-enabled credit card is being used, then the merchant server plug-in software can make a decision to skip authentication on the basis that the purchase request must be genuine and the cardholder details incorruptible.



And so a hybrid Stepwise-enabled 3D Secure transaction is radically simpler. The fact of cardholder enrollment in 3D Secure can be represented in the Stepwise capsule, removing the need for steps 2, 3,4 & 5. And by sealing the purchase request (1A) the browser proves to the Merchant server that the purchase request is genuine. The protocol demands that the Issuer still be sent a message (6) but if the PAReq extension is set, control reverts to the Merchant without delay, and without requiring any extra intervention by the user.



Stepwise hybridised with 3D Secure delivers the following benefits:

- it preserves the card schemes' investment in and commitment to 3D Secure, while improving the user experience

- it removes the two major bottlenecks and the off-putting pop-up box which leads to so much purchase abandonment

- it provides the familiar universal ATM-experience for home shopping

- it reduces the impact on merchants, and

- it improves security with genuine two factor authentication and resistance to Man in the Middle or replay attacks.

Stepwise "capsules" use standard digital certificates. The ability to handle extra certificates and digital signatures is part-and-parcel of the EMV standards. An EMV standard credit card chip can be loaded with the Stepwise "capsule" during personalisation with zero impact on the card schemes' security certification. Likewise, Stepwise utilises standard browser and merchant server software modules; Stepwise-enabling shopping cart software at the merchant side is very simple, and involves on the order of just 30 lines of code.

Lockstep Technologies has demonstrated the Stepwise solution, and developed a detailed architecture for integrating with 3D Secure. A technical whitepaper is available on request. We are planning a production pilot shortly.

Lockstep Technologies gratefully acknowledges G&D for providing the Innovation Seminar position.

http://lockstep.com.au/technologies