



Comparing Stepwise with other CNP fraud mitigations

The fundamental challenge in securing card transactions online is that a merchant server cannot tell if customer data presented remotely is genuine. Account details are being stolen and re-sold *en masse* by organised crime gangs that raid large merchants and processors in increasingly sophisticated attacks. The larger cases of credit card theft involve tens of millions of records. The recent court case against "Soup Nazi" hacker Albert Gonzales revealed that he stole over 130 million credit card records from Heartland Payment Systems, 7-Eleven and Hannaford Brothers.

Lockstep Technologies' *Stepwise* is an innovative solution to CNP fraud. As described in Tech Notes 2 and 3, *Stepwise* protects account details in a digital certificate issued to a chip device like an EMV smartcard. When a customer uses *Stepwise* to make a CNP payment, their details are bound to the transaction via a digital signature created in the chip, verifiable by the merchant server without referring to any intermediary.

Till now, there were two main responses to CNP fraud.

3D Secure

3D Secure is an online payments protocol developed by Visa and MasterCard (and marketed as *SecureCode* and *Verified by Visa* respectively). 3D Secure in essence tries to manage the risk of stolen account details by redirecting the shopper to the card issuer which then conducts a real-time repeat authentication to double check the cardholder's veracity. The repeat authentication is done by means chosen by the issuer, such as One Time Passcode, SMS message, a secondary static password and so on. Under 3D Secure rules, the Issuer accepts the risk of card fraud in the event that the extra authentication is somehow circumvented.

Acceptance of 3D Secure has been slow for several reasons. In particular it necessitates an extra enrolment step for cardholders, and it presents shoppers with an unusual, unnerving dialogue, often misinterpreted as a phishing attack. As a result, merchants report purchase abandonment rates of 50% or more.

Fundamentally, 3D Secure has a major impact on performance and business models. It complicates and slows down payment processing with several extra directions, and it joins the Issuer to the Cardholder for each transaction, in defiance of decades of credit card conventions.

Remote Chip Authentication

Remote Chip Authentication (RCA¹) makes use of the chip in an EMV card, and a standalone reader, to generate One Time Passcodes and challenge-responses which are re-keyed at participating shopping sites.

RCA necessitates verification of the onetime passcodes by a third party authentication server, and substantial re-keying between the reader and the browser. In contrast, *Stepwise* uses the EMV card in a connected reader to directly sign transactions in the browser, for better security, faster processing and greater customer convenience. RCA also suffers from a lack of interoperability between the readers and the cards of different banks.

Technologically, *Stepwise* and RCA are comparable in one respect: if a given EMV card can perform RCA transactions, then it will also be compatible with *Stepwise*.

The chief advantage of RCA is that its standalone readers are not vulnerable to key stroke logging malware. However, *Stepwise* is engineered to resist malware by intelligent means; details are available on application.

Other new approaches

End-to-end Encryption (E2EE) of cardholder details between merchant and card scheme networks protects data at rest at payment gateways and other intermediaries. E2EE restricts access by thieves at these points – which are amongst the major sources of stolen account details – but it cannot stop fraud re-using numbers stolen from other channels.

Tokenization replaces card numbers with unique reference numbers that cannot be re-used by fraudsters. However, it is a technically complex solution, entailing major back-end changes.

Stepwise

In contrast to RCA and 3D Secure, *Stepwise* is fast to process, supremely easy to use, and dramatically reduces the collection and exposure of personal data. No extra enrolment step is required. The architecture is uniquely elegant, simple to implement in existing merchant systems and with no impact on Acquirers. By targeting the specific vulnerability to replay of stolen account details, *Stepwise* preserves all other elements of conventional payment models, meaning it has the least possible impact on existing business rules, regulations and payment arrangements.

¹ RCA is marketed as *Card Authentication Protocol (CAP)* by MasterCard and *Dynamic Passcode Authentication* or (DPA) by Visa.