# Review and Commentary on "Closing the Phishing Hole – Fraud, Risk and Nonbanks" by Ross Anderson, April 2007

Rich Oliver
Retail Payments Product Manager
Federal Reserve System

## Summary

Mr. Anderson's paper examines the broad spectrum of contemporary payments fraud, accurately observing that the industry's move to electronic payments, coupled with the emergence of non-bank payments providers has significantly complicated the process of risk and fraud management. The author argues that efforts to mitigate fraud by focusing on identity have run their course and that the focus should shift to maximizing the revocability and recovery of funds.

My remarks are offered from the viewpoint of a payments system operator engaged in providing domestic and international automated clearing house (ACH) services. In the U.S., ACH has become a primary vehicle for clearing non-card based retail payments originated in several forms, including web and telephone based transactions. These venues, in particular, have become populated by a growing number of immoral (by someone's standards), if not illegal, businesses engaged in sub-prime lending, medical/pharmaceutical "services," gambling, and investment schemes.

Industry efforts to address this emerging "Wild West" environment have revealed a clear need for a balanced and multi-faceted program beginning with education and enhanced identification initiatives and proceeding through aggressive monitoring/progressive discipline (to include a "death penalty"), systems of fines and penalties, and an ambitious audit program. Moreover, it is critical that laws, regulations, and rule sets clearly place responsibility and liability on the party best situated to address problems.

With regard to the issue of revocability and recovery of payments to make aggrieved end users whole, there is also a balanced need to ensure that financial institution risk is managed by offering appropriate finality of payment rules.

In addition, it is not apparent that U.S. laws will be modified in the near-term to regulate non-bank third parties. I concur with the author's observation that these entities have developed useful innovations that have produced both efficient and convenient payments services for customers. Absent such legal reforms, it is incumbent on financial institutions and industry rule makers to "privatize" such controls through financial institutions networks.

## Discussion

The rapidly evolving environment of electronic payments is both a blessing and a curse. Electronification amplifies opportunities for securing and protecting data, as well as more systematically monitoring payment flows. The sophisticated "learning machines" employed by the card networks have become more and more adept at detecting and tracing fraud, sometimes based on a single transaction.

Alternatively, electronification has opened new doors to clever technologists to steal identities, falsify their own identities, and move money rapidly across the globe. Inevitably, the confluence of these phenomena has made it more and more difficult to identify and track fraudsters and their transactions, giving rise to a whole new field of payments forensics.

This evolution has resulted in a series of well intended, but spotty and reactive industry remedies, directed at addressing the latest problem to arise. In the U.S. ACH network, leaders and participants have begun to take a more comprehensive view, aided by recently adopted, and currently emerging, laws, regulations, and network rules.

As noted by Anderson, much attention has been paid to the early stages of identification. However, I believe that this focus has not run its course, at least not in the U.S. The requirements for dual factor authentication are just now being deployed on a widespread basis. Such controls, ultimately merged with biometrics as the costs of such solutions decline, will help frustrate fraudsters access to data. Further, a soon-to-be-adopted mandate to require companies to fully identify themselves and their customer service contact within the body of each debit transaction should enhance transparency and traceability.

Acknowledging that bad players may choose to still falsify their identity, ACH operators working together with the National Automated Clearing House Association[1] (NACHA) and bank regulators will actively monitor payment flows, looking for rapidly changing patterns of origination and unauthorized return items. Financial institutions experiencing such behavior will be counseled to investigate (and reform) badly behaving corporate customers.

Within NACHA rules, originating depository financial institutions (ODFIs) bear the responsibility and liability for the actions of their corporate originators. Continued inappropriate behavior will soon result in meaningful and escalating fines and penalties to the depository institution (DI) that should be passed on to the offending companies. Regular reports from operators will be the source of monitoring data and are available to DIs to encourage self monitoring. Should a DI fail to cooperate, their origination privileges could be revoked in the so-called “death penalty.”

Of course, the success of this scheme is supported by NACHA rules and Regulation E requirements that allow customers 60 days (two statement cycles) to return unauthorized transactions and be made whole. Assuming such transactions were truly unauthorized, the ODFI once again must stand good for the funds, thereby encouraging recovery from the originating company. Evidence exists that once burned, ODFIs become far more serious about underwriting standards, monitoring, and internal controls.

In summary, it is believed that further efforts at enhancing identification, coupled with more active monitoring and escalating penalties, will help exile bad players from the network and enhance the recoverability of funds, by allocating responsibility to the financial institution most able to deter fraud.

[1] NACHA is the U.S. rules and standards body for the ACH network. All participating financial institutions are bound to NACHA rules.