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

Roy DeCicco
Senior Vice President
Industry Issues Executive
JPMorgan Chase
Treasury Services
May 2, 2007

Professor Anderson places a high priority on the revocability and recovery of fraudulent payments. From the banking industry's perspective, there are important actions the industry should take once the facts of a fraudulent payment event are known. Most institutions in the payments business have a "fraud and protection" infrastructure that allows them to create aggressive actions to increase the likelihood that the proceeds of fraudulent transactions will be recovered. This infrastructure varies from institution to institution, but for most large payment banks, it includes specialists dedicated to loss recovery. These individuals work closely with legal and security subject matter experts to determine and execute recovery plans.

Bank payment providers place an equally high priority on fraud mitigation at the front-end of the payments cycle – providing services to reduce the likelihood that fraudulent transactions find their way into the payments system. To borrow a theme from Professor Anderson's paper, the industry's objective is to strengthen the safety and soundness of the payments infrastructure to a level where there is little or no economic incentive for the fraudsters to attack our payment channels. As you can imagine, this multi-faceted undertaking has many moving parts and many different players charged with helping us achieve the desired outcome.

The Importance of Customer Vigilance –

Key players would certainly include consumers or corporate entities that have access to payment channels through accounts that they control. I can not over state the importance that customer knowledge, awareness and vigilance play in ensuring security over a customer's accounts and the payment systems these systems use. The most secure payments system in the world will not mean a thing if customers are not vigilant and fall victim to phishing attacks and, in the process, gives up the security codes required to transact fraudulent payments. Customers can help protect themselves by:

- Being aware of the telltale signs of phishing schemes, such as typos or bad grammar,
- Being wary of embedded links in e-mails
- Using only trusted computers and
- Performing routine virus scans.

Many banks provide education and updates on sound business practices. Some banks offer web sites (such as abuse@chase.com) clients can use to report suspicious e-mails allegedly coming from the bank.

The Role of Industry Organizations –

Industry organizations, like BITS and NACHA, play an important role in examining the safety and soundness of our payment channels and determining the steps needed to minimize fraud in the payments environment.

The BITS Partner Group, an industry work group of financial institution, corporate and government subject matter experts, has examined cross-channel payments risk issues; this is critical given the propensity of fraudsters to move from channel to channel, following the path of least resistance. The Partner Group has developed proposals to promote data sharing, to close liability gaps and to develop standards for third party access control to payment systems. Additional industry action will be necessary to develop an implementation plan for those initiatives that gain industry consensus.

NACHA continues to implement a comprehensive risk management strategy that is meant to ensure high-quality ACH transactions and to mitigate risk for financial institutions, businesses and consumers by minimizing unauthorized entries and other exceptions. Rich Oliver will go into more detail on what the NACHA community is doing to maintain the highest possible safety and soundness standards within the ACH network.

Promoting Safety and Soundness –

I would like to focus on three aspects of what bank payment service providers are doing to promote safety and soundness and to mitigate fraud in the payments environment –

- Protecting clients' electronic credentials,
- Protecting clients' electronic transactions, and
- Empowering clients to manage user and access controls.

Protecting Clients' Electronic Credentials. Multi-factor authentication is being used to secure access to accounts and payment systems. Many industry experts describe the multifactor authentication process as a combination of using "something you know" (such as a password or PIN) along with "something you have" (such as a token/key fob or a registered PC (sometimes called a soft token or a machine fingerprint). Both the one time token device with a constantly changing code and the requirement to use a registered PC will thwart phishing.

More sophisticated three-factor authentication processes, which rely on "something you are" (such as a retina scan or a fingerprint) are available where the commercial rationale warrants such use. As the costs of these more sophisticated authentication processes come down, the market will see an increase in commercial applications.

More basic -- but equally as important -- are strong password guidelines that address length, complexity, expiration and freshness of passwords.

Protecting Clients' Electronic Transactions. For high risk transactions, some providers require a digital signature as a second level of authentication before payments can be released to a bank for processing. This process protects transactions from being intercepted and modified while being sent to the processing bank. The SecurID processes can also be time-based, providing an opportunity to manage the "time decay of trust." The principle behind this concept is that the longer the time from log-in to release of transactions, the less comfortable the paying bank will be with accepting those transactions for processing. Digital signatures serve to re-authenticate transactions for processing.

Banks are also developing capabilities to check clients' payment instructions against industry databases, such as those provided by Early Warning Services LLC, before finalizing the payments. This integration of information and technology is useful in the fight against fraud by providing bank payment service providers with current and accurate account-level information.

Empowering Clients to Manage User and Access Controls. This risk mitigant is focused on the electronic payments business that banks conduct on behalf of corporate clients. These security administration functions must be comprehensive and robust…and should include management of entitlements, limits and user activation.

Sarbanes-Oxley requirements have heightened corporate awareness of the need to manage access to payment systems. As a result, more corporate cash managers are "on the same page" as their bank payment service providers, and they look to these types of administrative functions to help them manage their user community.

Working Together To Manage Ongoing Risks –

The payments landscape is constantly at risk for fraud attacks. New threats, new adversaries and new tactics pop up every day. The level of sophistication increases with each new threat. This means that the broader industry – including bank providers, clients and industry organizations -- must each do their part to stay proactive and vigilant.

By working together, we can protect each other.