US ACH Payment Fraud: Myth or Reality?

George F. Thomas, Radix Consulting - 03 Aug 2010

What level of fraud exists in the ACH payment networks of the US? This article examines that question and looks at methods of fraud prevention.

Over the past year, there have been several highly publicised cases of corporate and government bank account takeovers. The thieves used the automated clearing house (ACH) network to initiate fraudulent credit transfers and then the wire transfer system to send the money from money mule accounts to the perpetrators offshore. The failure here was not a security vulnerability of the ACH network but was the result of either bank or corporate negligence. In many cases, banks had inadequate security controls for accessing the bank's cash management system allowing the customer accounts to be compromised. In other situations, business customers did not take advantage of the advanced access controls offered by their banks.

However, when it comes to payments system fraud, the king over the past five years has been the cheque collection system not the ACH network, according to the Payments Systems Fraud and Control Surveys conducted by the Association of Financial Professionals (AFP). The 2010 survey revealed that 73% of the companies surveyed experienced actual or attempted fraud, up 2% since the 2009 survey.[1] Of those companies that experienced actual or attempted fraud, 90% experienced attempted or actual cheque fraud. While the ACH was not immune from fraudulent attempts or actual fraud, ACH pales in comparison to cheque - the affected companies reported attempted or actual ACH debit fraud at 25% and ACH credit at 7%.

The ACH Infrastructure

The ACH offers a fast, inexpensive and reliable means of moving payments. It has also been a very safe payments mechanism for the majority of its 35-year history. Over the past five years, actual and attempted fraud has been managed reasonably well with attempts at ACH debit fraud dropping by 3% over the past year and ACH credit transfer attempts remaining constant at 7%.

The US ACH network operated by The Clearing House Payments Company under the product name Electronic Payments Network (46%) and the Federal Reserve Banks under the product name FedACH (54%) has operated safely and securely since the inception of the network without any fraudulent access or data breaches occurring through the network operators. So, I can say with the utmost confidence that the network that links all financial institutions within the US is extremely secure and safe.

The Weakest Link

Actual ACH fraud is at a very low level but, as we are all well aware, the ACH like any other payments network is only as secure as its weakest link. There are several factors that increase the risk of fraudulent ACH transactions:

Bank account information exposure

The first area of concern is the public exposure of bank account information. Every time a consumer or business issues a cheque it exposes its bank account information. The thieves understand how to interpret the MICR line on a cheque to acquire the bank account information. The account information is being used to fraudulently debit business and consumer accounts through the use of ACH debits and remotely created cheques.

The available solutions to this problem are the following:

- Eliminate cheque writing at the earliest possible opportunity.
- Promote the use of electronic payment credit transfers for consumers and businesses by securing the receivers' account information using the Universal Payment Identification Code (UPIC). UPICs maintain the security and privacy of the account information by masking it while facilitating the receipt of electronic payments. Business customers should ask their bank for a UPIC and the industry should start offering UPICs in the form of cell phone numbers to consumers.
- Business customers must take advantage of debit blocks and filters to prevent unauthorised debits to their accounts. Banks might look at the feasibility of offering these services to consumers as well. At least, to their private banking customers.

Bank due diligence

Attempted fraud and other illegal activities have resulted from ACH transaction types that have been implemented over the past 15 years. The newest forms of ACH transactions include internet authorised payments (WEB) and debits authorised over the telephone (TEL). These transaction types opened the door for those with illegal intent to use bank account information other than their own. It also created a prime environment for fraudulent telemarketers, illegal gambling and tobacco sales, child pornography and other illegal activities. Besides the ACH, the payment instrument of choice for fraudulent and illegal activity is now the remotely created cheque or demand draft.

While the newer ACH transaction types and use of demand drafts created the opportunity for increased risk, the risk was actually introduced by the poor due diligence practices of banks for Know Your Customer (KYC) and in the case of merchant payment processors, the absence of any procedures required by the bank for Know Your Customers' Customers (KYCC).

The solution for this problem is the implementation of enhanced due diligence procedures by the banks and verified by the appropriate regulators. Due diligence conducted properly by banks will go a long way in reducing fraudulent attempts on the ACH network.

Internet banking access

Earlier in the article I touched on company and government account takeover, in most of the known cases account fraud and identity theft are frequently the result of single-factor authentication that uses only user identification and password. For several years now, federal regulators have informed banks that use single-factor authentication as the only control mechanism that this practice is an inadequate security measure for high-risk transactions involving access to customer information or the movement of funds. Banks that offer internet banking products and services to their customers must use effective methods to authenticate the identity of customers accessing these systems. The regulators have indicated that authentication techniques employed by banks should be appropriate to the risks. It is imperative that banks offer and companies insist on multifactor authentication, layered security, or other controls designed to prevent account take-over.

The solution for this problem is the deployment of commercially reasonable multifactor authentication or layered security techniques that safeguard business and consumer bank accounts from account take-over scenarios. Banks can use are a variety of technologies and methodologies to authenticate customers. These methods include the use of customer passwords, personal identification numbers, digital certificates using a public key infrastructure, physical devices such as smart cards, one-time passwords, USB plug-ins or other types of ‘tokens’, transaction profile scripts, biometric identification, and security questions in combination with computer identification techniques.

An excellent example of a low-cost multifactor authentication technique can be found when accessing the Treasury Direct website. The Treasury’s method uses a series of access code cards, with passwords and access codes entered on random screen based keyboards to avoid programs that capture keyboard input.

Companies should demand multifactor authentication bank account access controls from their banks. If the bank does not offer advanced security techniques then the company needs to find a new bank.

Banks should also invest in front-end software that leverages the knowledge from past transactions and the application of business intelligence to detect attempts at fraud. The software would automatically alert the originating bank to possible man-in-the-browser and corporate account take over schemes by comparing all new ACH payments to previously processed transactions.

Conclusion

While the existence of ACH fraud is not a myth, it clearly is not at a sustainable level - US$100m in losses that the FBI estimates occurred in the most recent rash of account takeovers. It is a myth that these account take-overs only occurred at small and mid-sized financial institutions, customers of large financial institutions were impacted as well. The reality is that fraud in the ACH is not widespread and is being managed extremely well. It can be reduced even further by following the proposed solutions indicated in this article.

The facts are in - even though thieves will take advantage of any opportunity to exploit the payments systems, the electronic payment systems are much safer than using cheques. The banking industry must continually improve the security techniques necessary to protect their customer's accounts and funds; they can never become complacent because the thieves will make the most of any vulnerability that exists.

[1] Source: 2010 AFP Payments Fraud and Control Survey.