<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>3</td>
</tr>
<tr>
<td>THE ACH FRAUD PROCESS</td>
<td>3</td>
</tr>
<tr>
<td>FINDING THE NEEDLE IN THE HAYSTACK</td>
<td>5</td>
</tr>
<tr>
<td>LEGAL LANDSCAPE</td>
<td>5</td>
</tr>
<tr>
<td>THE CUSTOMER’S ROLE AND RESPONSIBILITIES</td>
<td>6</td>
</tr>
</tbody>
</table>
A recent press release from the National Automated Clearing House Association (NACHA) announced that in 2012, ACH volume in the United States increased by 4.19% to 21 billion transactions. That corresponded to a staggering $36.9 trillion in funds transferred, which represents an 8.76% increase over the amount transferred in 2011.

The increased adoption of ACH as a form of payment is not limited to the United States. Bacs, the United Kingdom’s equivalent to NACHA1, reported an increase in direct debit activity (ACH debit) from 2011 to 2012 of 3.23%. Across Europe, the blue book also reports growth in both credit and debit ACH transaction activity. Initiatives such as PE-ACH (pan-European ACH) also plan to consolidate domestic ACH switches and speed up the ability for customers to initiate payments across borders more quickly and conveniently. These types of initiatives will only serve as catalysts to increase the volume of ACH payments.

As ACH activity increases both in volume and value, so does risk and interest from cybercriminals and money launderers around the globe. This paper provides an overview of ACH fraud and compliance, including the tools and tactics cybercriminals use, the challenges facing banks and an outline of the framework that may help financial institutions reduce their exposure. The paper also includes an overview of recent legal disputes between banks and their commercial clients involving ACH and wire fraud.

Although the elements of each scheme will vary, electronic payments fraud, largely known as automated clearing house (ACH) fraud, typically involves the theft of a customer’s data via malware to facilitate the creation of unauthorized transfers or payment requests. Most of these payments are then subsequently laundered through mule accounts or established accounts that have been created by the criminal. Or they might target naive account holders who have been unwittingly convinced by the criminal that they are helping a legitimate cause for which they will also be remunerated once proceeds have been received.

As banks continue to improve their ability to detect ACH fraud, fraudsters continue to evolve their approach. For example, criminals who target small to large corporates may choose to submit a fraudulent ACH in an existing ACH batch file, or alter the previously designated payees and related amounts, hoping that the bank will not conduct a review of the batch for anomalies, modifications or additions. On a smaller scale, the criminal will initiate instructions requesting the bank to make regular low-value payments that can remain undetected by the genuine customer, but over time these payments can siphon off significant sums of money.
Other ACH and payment scams involve insurance and medical care. Criminals will set up regular payments with the insurance and medical care company and receive a service or, in turn, sell the procured service. Sadly, the service the criminal is receiving is being paid for by a genuine account holder who knows nothing about this transaction until they check their bank statement.

In general, an ACH fraud scheme involves the following steps:

• **Compromise customer data (low tech):** Gathering of customer information to complete a regular payment instruction. Typically, customer signature, branch routing or sort code, and account number. This type of information is easily acquired from a check transaction. Check volumes continue to fall globally, but they continue to be a source of useful intelligence for the criminal.

• **Compromise the customer’s computer (high tech):** Using phishing or spear phishing emails purporting to be from legitimate companies, fraudsters “trick” the recipient into providing their bank’s login credentials. By doing so, criminals capture the information that they need to access the customer’s account.

Malware, in the form of Trojans, viruses or worms are often used to infiltrate an individual or corporate computer unbeknownst to the end user, and can lay dormant until a financial transaction or access to financial information is initiated. So unlike the “tricked” recipient who actually provides login credentials, the malware can take over a session at any time and initiate fraudulent activity. Alternatively, criminals may use an insider to provide sufficient information to allow the criminals to take over an account.

• **Access the bank account online:** With the online login credentials in hand, criminals log into the customer’s bank account (manually or via malware code) and identify the account(s) to target.

• **Take over the account:** To avoid detection and the recall, or blocking, of pending ACH transactions, the fraudster may change the account holder’s email address, phone number, etc. and password.

• **Initiate ACH transactions:** With the account under their control, criminals initiate ACH transactions. Depending on the fraudster’s level of experience and need for funds, to avoid triggering the bank’s fraud detection rules, the fraudulent transaction amounts may appear consistent with the account holder’s previous transactions.

• **Respond to questions/attempts by the bank to verify legitimacy of transaction:** If the bank contacts the customer to verify the pending transactions, since the fraudster has changed the contact information on file, they may end up talking to a criminal who is pretending to be the customer. Alternatively, if the bank requests via email that the customer calls the bank to confirm the transaction, since the email on file is under control of the criminal, again, the bank will receive confirmation from the fraudster that the transactions are approved. Sophisticated software programs are also now available to intercept and redirect calls and emails so that they can be responded to (fraudulently) by the perpetrators.

• **Monitor account for receipt of funds:** Once the funds arrive in the fraudster’s account, time is of the essence. If a bank discovers the fraud quickly enough, they may be able to recall the funds. The quicker the funds leave the fraudster’s account — preferably for an international banking system — the lower the probability that the bank will recover the customer’s funds.

• **Layer funds to conceal the source:** To ensure that the fraudulent funds are impossible to recover, via a series of transactions including ACH, wire transfers and/or purchases, the fraudster conceals the source of the funds, or at least makes it extremely difficult to trace the funds to their ultimate destination.

• **Bust out:** Unpaid ACH transactions and returns can take up to 70 days, giving the fraudster ample time to carry out his plans. The fraudster can set himself up as a small business and initiate fraudulent ACH transactions, all based upon genuine customer routing (sort code) and account number details. The bust out fraudster could then withdraw the value and disappear prior to the ACH transactions being returned unpaid.

Regardless of the tools and tactics a bank deploys, criminals will make every attempt to overcome those countermeasures. According to the Association of Financial Professionals’, the typical loss associated with payments fraud in 2012 was USD$20,300 (this includes ACH debit, ACH credit, wire and commercial card payments). Quite simply, the rewards for committing ACH fraud are worth the effort.
With the volume of ACH transactions continuing to increase each year, to prevent ACH fraud, banks must find the proverbial needle in a haystack of legitimate transactions.

At each phase of the ACH fraud process detailed above, banks have the opportunity to prevent fraud. However, criminals also have the skills and expertise to thwart the bank’s efforts.

Ultimately, banks must balance the need to prevent fraud with their customers’ expectations that all electronic transfers take place “instantaneously.”

Typically, ACH fraud detection involves the following approaches:

- **Authentication**: Involves the comparison of data gathered from the customer such as user signature, name, password and something only the user knows, against information provided during the account opening phase or at some point during the life of the account. Additional factors may include tokens that generate random numbers the customer inputs, a USB device containing login credentials, or information about the customer’s device that the bank captures and associates with the account “behind the scenes.”

- **Risk-based approach**: Short-term, low-value, regular payment instructions (less than three months in duration) present a low risk to a financial institution if they turn out to be fraudulent. Financial institutions will have a threshold. Accumulative payments over a threshold will see stronger verification and authentication of the instruction. In this scenario, criminals will test, second guess the limits or harvest the intelligence from financial institution employees.

- **Account maintenance**: If a customer changes their phone number or email address, the bank contacts the customer via their mobile phone or secondary email address to confirm the customer did, in fact, make the request.

- **Customer behavior**: Behavioral profiling can be applied to monitor business or corporate accounts. For example, if a customer initiates ACH transactions using an unrecognized device that appears to be located overseas, software flags the account for further review.

- **Transaction monitoring**: Software reviews a customer’s activity for red flags, which are indicative of fraud. Transaction monitoring software captures data regarding the transactions, including the date and time requested, the payee account and name, the account number and the method used to initiate the ACH. If the bank suspects fraud, they may contact the customer directly to confirm the request. Creating profiles based on customer behavior over periods of time is also likely to be employed as part of a transaction monitoring solution. Profiling generally includes the usage of historical trends, previously identified fraud scenarios within a peer group and usual transaction amounts, etc., to minimize the frequency of false positives or unintended alerts regarding legitimate good customer behavior. Enhanced profiling activities can track statistics over a chosen time cycle for a financial or non-financial data element(s). These types of monitoring activities elevate the predictive nature of finding fraudulent activity.

- **Analytics**: Financial institutions often use advanced predictive analytic techniques to detect virtually all types of financial crime. Custom built (using the institution’s own known fraud data) or data from a consortium (using the collective data of many institutions) can provide additional intelligence to help in preventing fraudulent activity. Advanced analytics models can be particularly proficient at detecting obscure or less obvious patterns of behavior that are typically overlooked by human monitoring activities.

ACH and wire fraud schemes are similar in nature since they both involve unauthorized electronic payments. The following legal disputes involving ACH and wire fraud indicate that the courts have yet to apply a standard consistently to such disputes. (For additional information on the legal cases involving ACH and wire fraud, please see Volume 1 of the ACI fraud series, Fighting wire fraud: An industry perspective.)
CHOICE ESCROW AND LAND TITLE LLC VS. BANCORPSOUTH INC.³

In a dispute dating back several years involving an unauthorized wire of $440,000, the court sided with BancorpSouth. Cybercriminals stole the company’s login credentials and sent the wire to a corporate account in Cyprus. The bank previously offered the company dual control (two individuals must log in and approve the sending of a wire) and the company declined.

Verdict: The bank wins the case, primarily due to the customer’s refusal to implement additional security controls.

Note: Choice Escrow is appealing the court’s ruling.⁴

PATCO CONSTRUCTION COMPANY, INC. VS. PEOPLE’S UNITED BANK⁵

Several years ago, fraudsters captured a Patco employee’s login, password and answers to security-related questions. Via six ACHs, cybercriminals withdrew $588,851, of which $243,406 was recovered. The parties settled after protracted litigation. People’s United agreed to pay Patco for losses it suffered.

Verdict: The company settles with the bank after years of costly litigation.

VILLAGE VIEW ESCROW VS. PROFESSIONAL BUSINESS BANK⁶,⁷

After suffering a $393,000 net loss associated with 26 fraudulent wires, Village View Escrow sued Professional Business Bank. The owner of Village View Escrow stated that the bank normally notified her via email of each wire transfer associated with her account. The fraudsters apparently disabled this service before launching their attack. Using stolen passwords, the fraudsters provided two levels of approval required by the bank to release a wire.

Verdict: The bank agreed to reimburse the company for the loss and pay its legal fees.⁸

EXPERI-METAL VS. COMERICA⁹

District court in Michigan rules in favor of Experi-Metal for $561,399 in losses associated with a phishing attack. The judge determined that Comerica “had not operated in good faith with respect to its online banking protections.”

Verdict: Comerica reportedly settled with Experi-Metal for an undisclosed amount.¹⁰

4 THE CUSTOMER’S ROLE AND RESPONSIBILITIES

As the cases detailed indicate, the courts do not place the onus solely upon banks to prevent ACH fraud. Customers must also shoulder some of the burden. There are a number of steps that both individual customers and larger organizations and corporations need to make to minimize the risk of ACH fraud:

• Educate staff on the dangers of ACH: Companies should make sure that employees understand the potential damage that ACH fraud could inflict upon the company. To prevent employee compromise or collusion related to ACH fraud, they should subtly make all employees aware of some, but not all of the steps the company has in place to prevent internal fraud. The bottom line is to make employees understand that they need to be adhering to internal practices and policy which puts them in a position where they are not beyond reproach.

• Provide examples of fraudulent emails used to capture login information: Since many ACH fraud schemes begin with the introduction of malware, companies should provide employees with examples of fraudulent emails, as well as the steps to follow if they receive a suspicious email. In addition, the company should ensure that they have up-to-date anti-virus software deployed throughout their technology environment.

• Perform timely bank account reconciliations: Detecting ACH fraud requires that a company pay close attention to transactions posted to their account. Unfortunately, many companies don’t reconcile the activity in their account more frequently than once a month, or even once a quarter. By detecting the fraud long after the event, the bank cannot conduct an effective investigation or recover any of the customer’s funds.

• Signatures, routing and account numbers: Companies should be careful about releasing account details, particularly signatures, that could be used fraudulently to initiate regular payment instructions.

Finally, customers — both commercial and retail — should be made aware of the tools that the bank offers to prevent ACH fraud. Often customers are unaware that ACH fraud exists and that the bank can help protect their account.
ACH transaction volume continues to increase. Not surprisingly, so too do the attempts by criminals to initiate fraudulent ACH transactions. Both the bank and its customers play a role in ACH fraud prevention and detection. Educating customers on how best to prevent the introduction of malware that criminals use to capture login credentials can help prevent some instances of ACH fraud. However, customer education is just part of the solution. Fraudsters have a long list of tools and tactics to defeat the most highly educated and security-conscious organizations.

To combat ACH fraud, financial institutions must deploy a multi-layered approach that continually adapts to changes in the threat landscape. An intelligent fraud monitoring tool that analyzes and flags suspicious ACH transactions is crucial to detecting fraud, minimizing losses and ensuring the integrity of customer accounts.

As long as customers use the ACH system to transfer or initiate payments of funds, criminals will do their utmost to commit fraud. The sooner banks and their customers learn that the threat of fraud is here to stay, the better.

2 Association of Financial Professionals, 2013 AFP Payments Fraud and Control Survey, page 2
ACI Worldwide, the Universal Payments (UP) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers’ premises or through ACI’s private cloud, we provide real-time, immediate payments capabilities and enable the industry’s most complete omni-channel payments experience.

LEARN MORE

WWW.ACIWORLDWIDE.COM
@ACI_WORLDWIDE
CONTACT@ACIWORLDWIDE.COM

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide, Inc. 2017
ACI, ACI Worldwide, ACI Payment Systems, the ACI logo, ACI Universal Payments, UP, the UP logo, ReD, PAY.ON and all ACI product names are trademarks or registered trademarks of ACI Worldwide, Inc., or one of its subsidiaries, in the United States, other countries or both. Other parties’ trademarks referenced are the property of their respective owners.

ATL6316 05-17