

ACI's risk management software protects more than 150 financial institutions worldwide.

**Neshpal Manku**  
Manager, Global Help24, Bahrain

# Mitigating ACH and wire fraud perpetrated online

An industry article from ACI

While it's no surprise that fraud is on the rise due to the vast amount of sensitive data available to criminals through data breaches, phishing attacks and malicious code, what is alarming is the latest trend of automated clearing house (ACH) and wire fraud perpetrated through online banking channels as a result of access to sensitive account information.

## → A key piece of fraud intelligence strongly indicates that genuine customers tend to make transfers and bill payments to the same regular accounts and billers.

Despite the mass availability of sensitive account information available to criminals, there are steps that should be taken to seriously limit the exposure to ACH and wire fraud perpetrated online. This paper outlines ACH and wire fraud scenarios impacting financial institutions in recent months (both consumer and commercial accounts), as well as views on how this type of fraud can be countered and contained.

### **ACH and wire fraud scenarios**

The following scenarios describe two ACH and wire fraud trends recently impacting the financial institution industry:

#### **Scenario 1: Account takeover fraud**

**Step 1:** Fraudster opens a fake business account at bank A.

**Step 2:** Fraudster targets account holders at bank B through phishing attacks. Despite continual education on phishing, a certain percentage of bank B customers fall victim, and click on the phishing link, taking them

to a bogus site where they enter their login and authentication token information, which the fraudster captures.

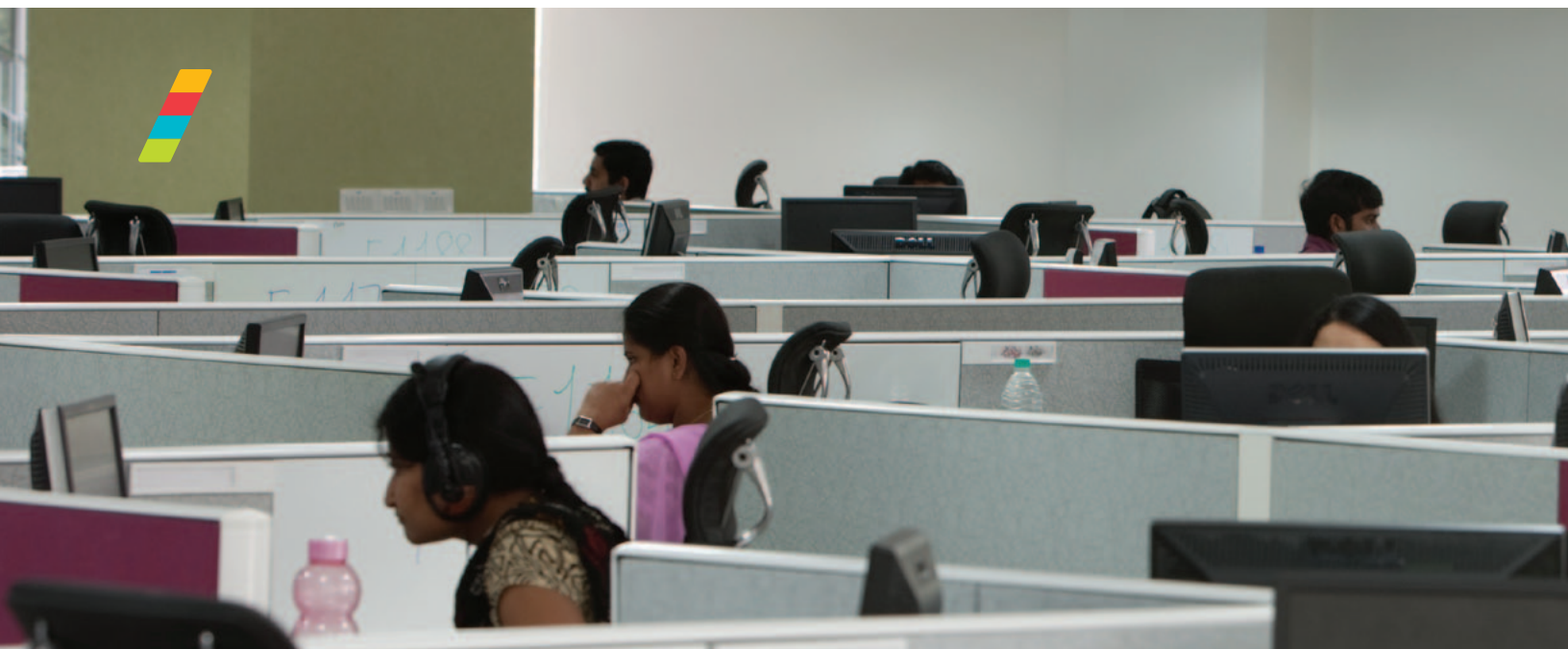
**Step 3:** Armed with sensitive account login and authentication token information, the fraudster accesses bank B's customers' online banking accounts.

**Step 4:** Once inside the online banking system, the fraudster initiates an ACH transaction to the fake business at bank A.

**Step 5:** Once the funds have been transferred to bank A, the fraudster then initiates a wire transfer from the fake business account (at bank A) to bank C (either domestic or foreign).

#### **Scenario 2: Man-in-the-middle attacks**

**Step 1:** Fraudster writes malicious code (hidden in email spam scams, such as fake news stories, popular videos, links to greeting cards, etc.), which infects account holders' computers with a virus that collects data typed into web forms, including banking pages.



**Step 2:** Armed with data entered into the web forms, the fraudster utilizes a spear-phishing campaign to target the specific accounts with recent online banking activity, sending them a highly personalized and convincing email asking them to “click here” to reset their security code, which installs another virus that waits for their next online banking session.

**Step 3:** The next time an account holder logs into their online banking account, the fraudster’s virus inserts itself between them and their online banking system, where it executes commands to initiate wire transfers or ACH transactions unbeknown to the genuine account holder.

#### **Benefits and limits of multifactor authentication**

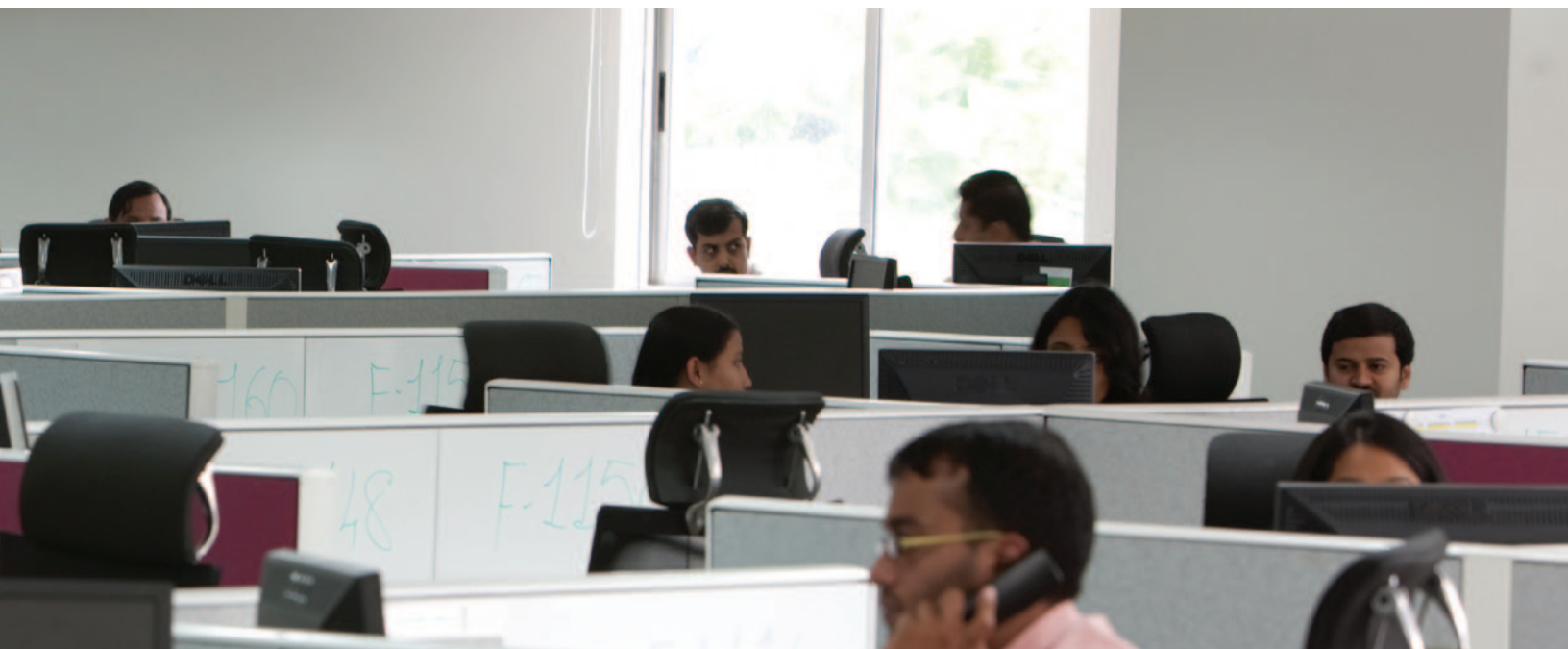
One approach to prevent ACH and wire fraud perpetrated online is through the use of two-factor or multifactor authentication methods. These can range from tokens on key fobs to one-time passwords delivered via Single Message Service (SMS).

The downside to this approach is that the cost and customer inconvenience involved often make this approach prohibitive: supplying an entire customer base with tokens that can break or be lost often becomes an expensive exercise. Additionally, as described by the two previous scenarios, fraudsters continue to find their way around authentication measures through phishing attacks and malicious code.

#### **Transactional monitoring and customer profiling**

Because customer authentication measures sometimes fall short, financial institutions can mitigate their risk by monitoring transactional behavior to determine whether or not ACH and wire activity occurring online fits the profile for the genuine customer.

Non-financial indicators – such as IP addresses, session IDs, account maintenance activities, password changes, path tracking, etc. – have become the dominant indicators of fraudulent activity and should be used to create a customer profile.





All customer interactions can be categorized into event classes that incorporate both monetary and non-monetary actions. These are as follows:

- **Payment events:** Financial transactions such as funds transfers and bill payments
- **Login events:** IP address and session ID profiling
- **Password events:** Changes in logon passwords
- **Profile events:** Changes to customer demographic information (e.g., addresses)
- **Payee events:** Changes to external payee account details
- **Navigation events:** Changes to how a customer navigates an online internet portal

In isolation, one of these events may not indicate fraudulent activity. When combined, however, they predict strong patterns of criminal intent.

A key piece of fraud intelligence strongly indicates that genuine customers tend to make transfers and bill payments to the same regular accounts and billers. Alternatively, fraudsters will transfer money to an account or biller that the genuine customer has never used. Account profiling is a technique that enables institutions to cross-reference all external accounts with which a customer has transacted in the last 12 months against each new transfer. When a transfer occurs to

an account the customer has never used before, the institution should analyze that transaction in greater detail.

Another powerful indicator of online banking fraud is analyzing the login event – particularly IP address profiling. A static IP address provides each computer a unique identifier on the internet. Once a series of online accounts has been compromised, fraudsters often log in from a single location to illegally transfer funds. The criminal's IP address should be captured and maintained in a negative list, and any future login attempts from blacklisted IPs should automatically decline access to the fraudster, effectively preventing fraud. Financial institutions should establish an expected IP address footprint for customers and therefore identify which internet banking logins and transactions to treat as potentially suspicious.

When high risk activity is detected, action can be taken in real time or near real time to stop the transfer of funds from the customer's account. Funds can be placed on hold until fraud analysts are able to verify the legitimacy of the transaction. Monitoring ACH and wire activity occurring online not only saves money by reducing overall fraud loss, it also provides reputational risk protection that has an incalculably priceless value.



#### **ACI Worldwide**

Offices in principal cities throughout the world  
[www.aciworldwide.com](http://www.aciworldwide.com)

Americas +1 402 390 7600

Asia Pacific +65 6334 4843

Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide 2010

All product names are trademarks or registered trademarks of their respective companies. ACI and the ACI logo are trademarks or registered trademarks of ACI Worldwide Corp. in the United States, other countries, or both.

ATL4398 10-10

#### **About ACI Worldwide**

ACI Worldwide powers electronic payments for financial institutions, retailers and processors around the world with the broadest, most integrated suite of electronic payment software in the market. More than 75 billion times each year, ACI's solutions process consumer payments. On an average day, ACI software manages more than US\$12 trillion in wholesale payments. And for more than 150 payments organizations worldwide, ACI software ensures people and businesses don't fall victim to financial crime. We are trusted globally based on our unrivaled understanding of payments and related processes. We have a definitive vision of how electronic payment systems will look in the future and we have the knowledge, scale and resources to deliver it. Since 1975, ACI has provided software solutions to the world's innovators. We welcome the opportunity to do the same for you.