

# NACHA Risk Management News

Volume 6, Issue 1

## **Chrystina Giorgio Leads NACHA's Risk Management Advisory Group into 2010**



**S**imple. Safe. Secure. That is the tagline used to describe the ACH Network. As an industry, we have done a tremendous job keeping the Network safe and secure thanks to a collective effort by NACHA's Risk Management Advisory Group (RMAG) and our partners at the Regional Payments Associations, the Federal Reserve, and EPN. In these times of increasing Trojan viruses, malware, phishing and numerous other cyber threats, we cannot rest on our laurels. Instead, we must continue to work together to share experiences, knowledge, and expertise to combat the ever evolving threats to our business. These efforts do not stop with NACHA or RMAG – these are the starting points. With every Network participant's diligence, we can be successful at mitigating the risks we will continue to face.

Over the past twelve months, numerous initiatives have been implemented to protect the Network; and many of these initiatives began with RMAG, like the Risk Management and Assessment and Direct Access Registration Rules, both slated for implementation in 2010. Some initiatives were designed to help participants develop best practices in their own organizations around third parties and origination.

I congratulate RMAG for their efforts and thank them for their service to the industry.



Chrystina Giorgio

As we look to 2010 and beyond, we will continue to focus on origination risks and mitigation tools. Applications for financial institutions to enable them to share information to allow for better due diligence through applications such as the currently piloted Originator Watch List and the concept of a Terminated Originator Database, will enable the highest risks to be identified and aid in the mitigation of such risks.

As we embark on these initiatives, I hope we can continue to work collaboratively for the good of all stakeholders in the ACH Network.

*Chrystina Giorgio is Senior Vice President, Deposit Operations at Sandy Spring Bank in Columbia, MD.*

### Inside this issue:

<b>Direct Access Registration</b>	2
<b>ODFI Best Practices—Two Recent ACH Risk Management White Papers Released</b>	4
<b>The National System of Fines—Working For You!</b>	6
<b>Corporate Account Takeover</b>	7
<b>NACHA's Risk Management Advisory Group</b>	9

### NACHA Risk Management News

is a publication of

NACHA—The Electronic Payments Association  
13450 Sunrise Valley Drive  
Suite 100  
Herndon, VA 20171  
Phone: 703/561-1100  
Fax: 703/787-0996

© 2010 National Automated Clearing House Association  
All rights reserved.

## Direct Access Registration

### Rule Requires ODFIs to Act by June 18, 2010

The NACHA Board of Directors approved a policy statement on July 30, 2008 expecting DFIs to register their Direct Access Debit Relationships with NACHA and to follow prudent risk mitigation techniques—including adherence to best practices—for the duration of those relationships. While the Direct Access registration effort via the NACHA Board Policy proved effective, it did not provide enough incentive to inspire all ODFIs to register. In addition, under the current Policy, there are no enforcement abilities under the National System of Fines when an ODFI does not register.

The potential impact of Direct Access relationships has long been the subject of discussion within the ACH Network and the impetus to codify the 2008 Board policy into a provision in the *NACHA Operating Rules (Rules)*.

***The Direct Access Registration Rule requires an ODFI to register its Direct Access status with NACHA by June 18, 2010.***

**Direct Access** is a situation in which an Originator, Third-Party Sender, or a Third-Party Service Provider transmits credit or debit entries to an ACH Operator using the ODFIs routing and transit number and settlement account.

**Direct Access Debit Participant** is an Originator, Third-Party Sender, or Third-Party Service Provider with Direct Access for the origination of entries except (i) a Third-Party Service Provider that transmits ACH files solely on behalf of an ODFI where that Third-Party Service Provider does not have a direct agreement with an Originator (and is not itself an Originator), or (ii) an ODFI that transmits files using another Participating DFI's routing number and settlement account.

When an ODFI allows Originators, Third-Party Service Providers or Third-Party Senders Direct Access to the ACH Operators, ACH Network participants, including the ODFI, may be exposed to risks arising out of shortcomings in the Originator's or third party's policies and processes.

Accordingly, it is essential that an ODFI that permits Direct Access effectively mitigate such risks by appropriately underwriting, managing, and monitoring the relationship with its customer. ACH Operator tools that allow tracking of volume and exceptions are available to assist ODFIs in these efforts.

Regardless of the level of due diligence performed by the ODFI's Direct Access customers, the ODFI remains responsible for those customers and for the entries they introduce into the Network.

#### **ODFIs with Direct Access Debit Participants**

An ODFI that has Direct Access relationships for debit origination (*Direct Access Debit Participants*) is required to:

- Provide NACHA with specific information about each Originator or third party with Direct Access, as well as data about that party's transaction volume.
- Provide specified transaction data on a quarterly basis via the registration process.

The Rule also requires an ODFI's board, committee of the board, or the board's designee to approve a Direct Access Debit Participant prior to the origination of ACH debit entries for that Participant. (This applies to relationships that are established on or after June 18, 2010.)

(Continued on Page 3)

## Direct Access Registration (Cont'd)

An ODFI is further required to report when there is a change in the information provided during registration for a current Direct Access Debit Participant, including termination of a relationship.

### **ODFIs with No Direct Access Debit Participants**

An ODFI with no Direct Access Debit Participant relationships is required to acknowledge a statement to that effect by June 18, 2010.

### ***Where do Financial Institutions go for more information?***

Direct Access forms and more information on the registration can be found at:

<http://www.nacha.org/OtherResources/riskmgmt/DirectAccess/default.htm>

***NOTE - ODFIs that have already registered their Direct Access status with NACHA under the Board policy do not need to re-register to be compliant with the rule requirement. ODFIs that have already registered will only need to provide updates and changes as appropriate.***

**For more information on Direct Access Registration or any ACH risk-related issue, contact NACHA staff below:**

#### **NACHA Risk Investigations and Services**

**Deborah Shaw, AAP, CTP**

Managing Director  
dshaw@nacha.org or 703-561-3919

**Jeanette A. Fox, AAP**

Senior Director  
jfox@nacha.org or 703-561-3914

**Lisa Newhall**

Assistant Director  
lnewhall@nacha.org or 703-561-3968

**Cathy McNickle**

Manager  
cmcnickle@nacha.org or 703-561-3959

## NACHA's Teleseminar Series

### **NACHA Operating Rules Change—Rules Audit Enhancement**

**February 10, 2010, 1:30 p.m.—3:00 p.m. Eastern Time**

This Rule change became effective December 18, 2009 and is applicable to annual audits to be conducted by December 1, 2010. The Rules Audit Enhancement Rule promotes more effective annual audits of compliance with the *NACHA Operating Rules* by participating Depository Financial Institutions (DFIs) and facilitates compliance with the *Rules* that ultimately leads to lower risk and higher quality in the processing of ACH payments. This rule refines and clarifies existing *Rules* compliance audit requirements for all DFIs with specific provisions for ODFIs and RDFIs.

**Register for this teleseminar at this link:**

[http://www.nacha.org/conferences/teleseminars/Tele\\_021010/index.html](http://www.nacha.org/conferences/teleseminars/Tele_021010/index.html)

### **NACHA Operating Rules Change—Risk Management & Assessment**

**March 10, 2010, 1:30 p.m.—3:00 p.m. Eastern Time**

This rule change becomes effective June 18, 2010.

The Risk Management and Assessment rule will codify within the *NACHA Operating Rules* additional risk management practices that are common in the industry and help improve risk management in the ACH Network. This rule requires:

- DFIs to conduct a risk assessment of their ACH activities in accordance with the requirements of their regulator(s);
- ODFIs to incorporate certain topics into their agreements with Originators and Third-Party Senders; and
- ODFIs to perform a more comprehensive set of risk management practices, including financial and operational due diligence on Originators, assessing the risks of Originator's activity; monitoring origination and return activity; enforcing restrictions on exposure limits; and enforcing restrictions on the types of ACH transactions that may be originated.

**Register for this teleseminar at this link:**

[http://www.nacha.org/conferences/teleseminars/Tele\\_031010/index.html](http://www.nacha.org/conferences/teleseminars/Tele_031010/index.html)

## **ACH Risk Management White Papers - Two Papers Offer Best Practices for ODFIs**

NACHA's Risk Management Advisory Group (RMAG) recently issued two white papers that provide ODFIs in the ACH Network guidance on two very important subjects—originating in challenging economic times and Third-Party Sender risk.

---

### ***ODFI Best Practices for Originating ACH Transactions (September 2009)***

RMAG sponsored a survey in April 2009 titled, *ODFI Best Practices for Originating ACH Transactions in Challenging Economic Times*. One hundred sixty-three ODFIs responded to the survey offering insight into current ACH origination practices.

Following the survey, RMAG completed a white paper, *ODFI Best Practices for Originating ACH Transactions*. In addition to an analysis of the survey results, the white paper also relates the ODFIs' responses to provisions of the *2009 NACHA Operating Rules (Rules)*, as well as the Office of Comptroller of the Currency (OCC) Bulletins 2006-39, *Automated Clearing House Activities: Risk Management Guidance* and 2008-12, *Payment Processors: Risk Management Guidance*.

The white paper includes recommendations for sound risk management practices including, but not limited to, the following practices.

#### ***Employ a multi-faceted approach to underwriting Originators***

- OCC Bulletin 2006-39 includes a section on establishing Originator underwriting standards that lists background checks as a component of sound underwriting standards.

#### ***Seek objective, unbiased information about Originators***

- Public Web sites and open source research provide some useful information; however, ODFIs should understand that some sites contain information that comes directly from the entity being profiled. In such cases, the information may include a biased opinion rather than objective facts. That does not imply that the information is necessarily incorrect, just that an ODFI performing a background check should consult more than one source in order to corroborate information about an Originator.

#### ***Know details about all participants related to third-party relationships***

- OCC Bulletin 2006-39 addresses the need for ODFIs to know details about all participants in third-party relationships by indicating that financial institutions "should know, at a minimum, for which Originators they are initiating entries into the ACH Network. ODFIs should require Third-Party Senders to provide certain information on their Originator customers such as the Originator's name, taxpayer identification number, principal business activity, and geographic location. Also, before originating transactions, a bank should verify (directly or through a Third-Party Sender) that the Originator is operating a legitimate business."

#### ***Monitor credit exposure across multiple settlement dates***

- This is an explicit requirement in the *Rules*, clearly spelled out as a prerequisite to origination in Article Two, Subsections 2.1.12, ODFI Exposure Limits, and 2.12.2.3, ODFI Exposure Limits. The OCC Guidance echoes this with equal clarity, saying that banks should also implement procedures to monitor ACH entries relative to the exposure limit across multiple settlement dates."

(Continued on Page 5)

## ACH Risk Management White Papers (Cont'd)

### **Recognize that risk exposure related to an Originator spans payment channels and review policies and practices periodically as the business environment changes.**

- OCC Bulletin 2006-39 suggests that bank management should “require lending and ACH operations personnel to consult with one another at least annually to confirm that the Originator’s financial condition has not changed from the time the credit facility was approved.”

### **Review policies and practices periodically as the business environment changes.**

- ODFIs must understand that a periodic re-evaluation should consider more than just creditworthiness and should consider risk factors such as changes in lines of business, changes in market condition, or changes in service.

---

### **Third-Party Sender Case Studies: ODFI Best Practices to Close the Gap (December 2009)**

ODFIs face unique challenges and potential risks in Third-Party Sender relationships. To mitigate risk, it is critical that ODFIs fully understand their responsibilities and inherent risks in third party relationships. A second RMAG white paper, *Third-Party Sender Case Studies: ODFI Best Practices to Close the Gap*, illustrates potential risks to ODFIs in Third-Party Sender relationships.

Third-Party Sender relationships may not be right for every financial institution. A financial institution must assess whether Third-Party Sender relationships fit into the financial institution’s payments strategy and culture and whether the financial institution has both people and processes in place to manage the risk of Third-Party Senders appropriately.

ODFIs should consider best practices and carefully review their obligations and liabilities under the *Rules* for Third-Party Senders so that their agreements

appropriately reflect these issues as they bring on a new, or review an existing Third-Party Sender relationship.

### **Verify basic facts**

- An ODFI has an obligation to request and verify basic facts such as Name, DBAs, Address, Tax ID, Principal’s Name(s), and type of business or activity.

### **Conduct due diligence**

- An ODFI should perform due diligence to understand the third party’s business activities. Due diligence should include, but not be limited to, confirmation of the existence of a Web site and a review of any associated advertising, marketing, scripts, products and services. Also perform a site visit if possible. Request and verify business references. Perform open source research on the Internet. Consult resources such as Dun & Bradstreet and the Better Business Bureau. Obtain historical rates of return for the third party and each of its Originators.

### **Ensure agreements cover all necessary provisions**

- The ODFI needs to ensure that their Third-Party Sender has an agreement with its Originators. Agreements should define all responsibilities, policies and procedures, including provisions to ensure that the third party and each of its Originators operate within compliance with the *NACHA Operating Rules*. Agreements should also identify prohibited business lines and define termination policies and procedures.

### **Perform regular reviews**

- An ODFI should perform a regular review of the financial condition and credit reports of the principal(s) of the Third-Party Sender. Take a risk-based approach to the third party’s activities and individual Originator’s activities. This includes monitoring activity, reviewing SEC Code use and associated authorization methods used, return rate monitoring, and investigating any complaints or concerns made by other financial institutions or peer organizations.

## The National System of Fines—Working for YOU!

NACHA's National System of Fines is a process that allows participating financial institutions to submit a Report of Possible ACH Rules Violation to NACHA when a party to an ACH transaction believes that there has been a violation of the *NACHA Operating Rules (Rules)*. While the National System of Fines is used by many financial institutions, some do not use it—perhaps under the notion that the process is complicated and time consuming.

Good news for ACH Network participants – NACHA is automating the process! NACHA is currently testing the automated submission process, which will allow financial institutions to complete and submit a Report of Possible ACH Rules Violation online in a secure environment. Users will be able to upload supporting documentation, eliminating the need to fax or mail these documents. This new process is intended to reduce the time and expense associated with submitting a Report of Possible ACH Rules Violation, and will also provide users with confirmation of submissions.

The ACH Network is a truly ubiquitous payment system, reaching over 15,000 financial institutions. Over 18 billion transactions were processed in 2008, and the volume for 2009 will be commensurate with prior year's increases. With volumes at these levels, it is no surprise that problems and issues may occur. No matter the reason, deviations from the *Rules* cost financial institutions time and money to resolve. Financial institutions have to handle rejects and exceptions, which result in increased costs that are directly associated with customer service calls, Written Statements Under Penalty of Perjury, research, manual processes and returns.

The *Rules* require a financial institution or ACH Operator that is a 'party to the transaction' to submit a Report of Possible ACH Rules Violation to NACHA. In other words, every participating financial institution

has a responsibility to ensure that the ACH Network is safe, secure and reliable. If users do not report possible violations of the *Rules*, no action can be taken under the National System of Fines to resolve the Issue.

### When Should You Submit a Report of Possible ACH Rules Violation?

The answer is—when your institution sees a serious or ongoing violation of the *Rules*. Specific examples include situations involving:

- Non-response to Notifications of Change
- Unauthorized Entries
- Failure to provide Copy of Authorization
- Failure to Provide Copy of WSUPP
- Ineligible Source Documents
- Exceeding Reinitiation Limits
- Improper SEC Code Use
- Untimely Returns

### Do Your Part to Improve ACH Network Quality

Please don't rely on other financial institutions to do the heavy lifting. If everyone does their part in submitting Reports of Possible ACH Rules Violation, the National System of Fines can work to address compliance issues. NACHA is doing their part to make the process more efficient, but it takes participating financial institutions to make the process truly effective.

#### NACHA Network Compliance Contacts

**Lorie Nash, AAP**

**Senior Director**

**[lnash@nacha.org](mailto:lnash@nacha.org) or 703-561-3917**

**Brenda McGuiney, AAP**

**Director**

**[bmcguiney@nacha.org](mailto:bmcguiney@nacha.org) or 703-561-3956**

# Corporate Account Takeover

## These Cyber Schemes Can Lead to Fraudulent Transactions

The following excerpt is taken from the recent NACHA Operations Bulletin issued December 2, 2009. For the complete Bulletin, go to: [www.nacha.org](http://www.nacha.org).

### WHAT IS CORPORATE ACCOUNT TAKEOVER?

“Corporate account takeover” is when cyber-thieves gain control of a business’ bank account by stealing the business’ valid online banking credentials. Although there are several methods being employed to steal credentials, the most prevalent involves malware that infects a business’ computer workstations and laptops.

A business can become infected with malware via infected documents attached to an e-mail or a link contained within an e-mail that connects to an infected Web site. In addition, malware can be downloaded to users’ workstations and laptops by visiting legitimate Web sites - especially social networking sites - and clicking on the documents, videos or photos posted there. This malware can also spread across a business’ internal network.

In a recent attack, cyber-thieves sent millions of e-mails purporting to come from NACHA. Mimicking a reputable, national organization is a common tactic used by cyber-thieves to gain credibility and lure unsuspecting individuals into taking some action. The e-mail “reported” a rejected ACH transaction, and included a link for an “Unauthorized ACH Transaction Report.” A recipient who clicked on the link would be taken to a fake Web site that mimicked the real NACHA Web site, which prompted the recipient to click on a fake transaction report. If the recipient clicked the link, the malware was downloaded to the recipient’s computer.

The malware installs keylogging software on the computer, which allows the perpetrator to capture a user’s credentials as they are entered at the financial institution’s Web site. Sophisticated versions of this malware can even capture token-generated passwords, alter the display of the financial institution’s Web site to the user, and/or display a fake Web page indicating that the financial institution’s Web site is down. In this last case, the perpetrator can access the business’ account online without the possibility that the real user will log in to the Web site.

Once installed, the malware provides the information that enables the cyber-thieves to impersonate the business in online banking sessions. To the financial institution, the credentials look just like the legitimate user. The perpetrator has access to and can review the account details of the business, including account activity and patterns, and ACH and wire transfer origination parameters (such as file size and frequency limits, and Standard Entry Class (SEC) Codes).

The cyber-thieves use the sessions to initiate funds transfers, by ACH or wire transfer, to the bank accounts of associates within the U.S. These accounts may be newly opened by accomplices or unwitting “money mules” for the express purpose of receiving and laundering these funds. The accomplices or mules withdraw the entire balances shortly after receiving the money, and then send the funds overseas via over-the-counter wire transfer or other common money transfer services.

### WHY ARE SMALLER BUSINESSES AND ORGANIZATIONS TARGETED?

The cyber-thieves appear to be targeting small- to medium-sized businesses, as well as smaller government agencies and non-profits, for several reasons:

- Many small businesses and organizations have the capability to initiate funds transfers - ACH credits and wire transfers - via online banking (individual consumers generally do not have this capability except for payees set up in online bill payment systems). This funds transfer capability is often related to a small business’ origination of payroll payments.

In corporate account takeover, the cyber-thieves may add fictitious names to a payroll file (directed to the accounts of money mules), and/or initiate payroll payments off-cycle to avoid daily origination limits.

(Continued on Page 8)

## Corporate Account Takeover (Cont'd)

- Small businesses often do not have the same level of resources as larger companies to defend their information technology systems.
- Many small businesses do not utilize additional banking services, such as password-generating tokens, and do not monitor and reconcile their accounts on a frequent or daily basis.
- Ensure that all anti-virus and security software and mechanisms for all computer workstations and laptops that are used for online banking and payments are robust and up-to-date.
- Restrict functions for computer workstations and laptops that are used for online banking and payments. For example, a workstation used for online banking should not be used for general Web browsing and social networking. A better solution is to conduct online banking and payments activity from a dedicated computer that is not used for other online activity, and/or is not connected to an internal network.

### WHAT CAN A FINANCIAL INSTITUTION DO?

Financial institutions and business customers have distinct responsibilities to help address the security of online access to businesses' accounts. Each can take steps to protect corporate accounts from being taken over.

The top things financial institutions can do are:

- Deploy multi-factor and multi-channel authentication for business accounts that are permitted to initiate funds transfers. For example: something the person knows (user ID, PIN, password) and something the person has (password-generating token, USB token).
- Require their business customers to initiate payments under dual control, with distinct responsibility for transaction origination and authorization.
- Enable "out-of-band" confirmation of payment initiation, or for certain defined types of payments.
- Provide out-of-band alerts for unusual activity ("red flag" reports).
- Establish and monitor exposure limits that are related to customers' activities.
- Monitor and reconcile accounts daily. Many small business clients do not reconcile their bank accounts on a daily basis, and therefore may not recognize fraudulent activity until it is too late to take action.
- Utilize routine and "red-flag" reporting (i.e., alerts about unusual activity) for transaction activity.

Financial institutions should educate their business customers on prevention, detection and reporting measures. The top things a business can do are:

- Initiate ACH and wire transfer payments under dual control. For example: one person authorizes the creation of the payment file and a second person authorizes the release of the file.
- Contact appropriate law enforcement immediately.
- Contact the RDFI(s) to determine if the funds have been withdrawn and to work on options for recovery.
- File a Suspicious Activity Report.
- Conduct a forensic analysis and consider suspending the business' funds transfer capabilities until the results are known.

### ACH OPERATOR SERVICES

Financial institutions should consider fraud detection and risk management services offered by their ACH Operators. For example, a threshold or a cap on ACH credit origination could alert a financial institution, particularly a small institution with low average daily ACH credit origination, to irregular origination activity.

### WHAT TO DO IF YOUR CUSTOMER IS VICTIMIZED

A financial institution whose customer has been victimized can do the following.

## NACHA's Risk Management Advisory Group

**Chrystina M. Giorgio, AAP**  
Sandy Spring Bank  
*RMAG Chairperson*

**Christopher Alexander, AAP**  
Federal Reserve Bank of Atlanta

**Patricia Campbell**  
Christian Financial Credit Union

**Keith Crockett**  
BBVA Compass

**Roy DeCicco, CCM**  
J.P.Morgan

**Joseph Flannery, AAP**  
BB&T

**Barry Gideon, AAP**  
First National Bank of Omaha

**Steven J. Helgen**  
U.S. Bank

**Daniel J. Heller**  
Wells Fargo

**Peter C. Hohenstein, CCM**  
Bank of America

**Ron Kiefer**  
City National Bank

**Fred Laing II, AAP, CCM**  
Upper Midwest ACH Association

**Tom Masterson**  
The Clearing House LLC

**Sara Pinkus, AAP**  
TD Bank

**Rayleen Pirnie**  
EPCOR

**Pamela Rodriguez, AAP, CIA, CISA**  
EastPay Inc.

**Michelle Sledge, AAP**  
Fifth Third Bank

**Samuel A. Vallandingham**  
The First State Bank

**Steve Whitney**  
Norway Savings Bank

### NACHA's RISK MANAGEMENT STRATEGY

NACHA's Risk Management Strategy strives to balance risk mitigation initiatives with quality enhancements to ensure that sound, practical and effective solutions are achieved.

