

NACHA Risk Management News

Direct Access Registration — ODFIs Must Register by June 18, 2010

The Direct Access Registration rule requires all ODFIs to register their Direct Access status with NACHA no later than June 18, 2010.

ODFIs that have already registered their Direct Access status with NACHA do not have to register again unless their Direct Access status changes.

Direct Access Registration promotes due diligence and adherence to risk management policies by ODFIs. Registration also allows for an accurate measurement of the number of Direct Access relationships in the ACH Network and the associated risk profile.

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 Debit Participants is required to:

- Provide NACHA with specific information about each Originator or third party with Direct Access.
- Provide specified transaction data on a quarterly basis.

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.)

Welcome to PAYMENTS 2010

Inside this issue:

| | |
|--|----------|
| Risk Management and Assessment Rule | 3 |
| Cyber Schemes Lead to Fraudulent Transactions | 4 |
| Risk Management Advisory Group Initiatives Update | 6 |
| Risk Management Advisory Group Participants | 7 |
| Payments 2010 Risk-Related Sessions Highlighted | 8 |

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 Requirements (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.

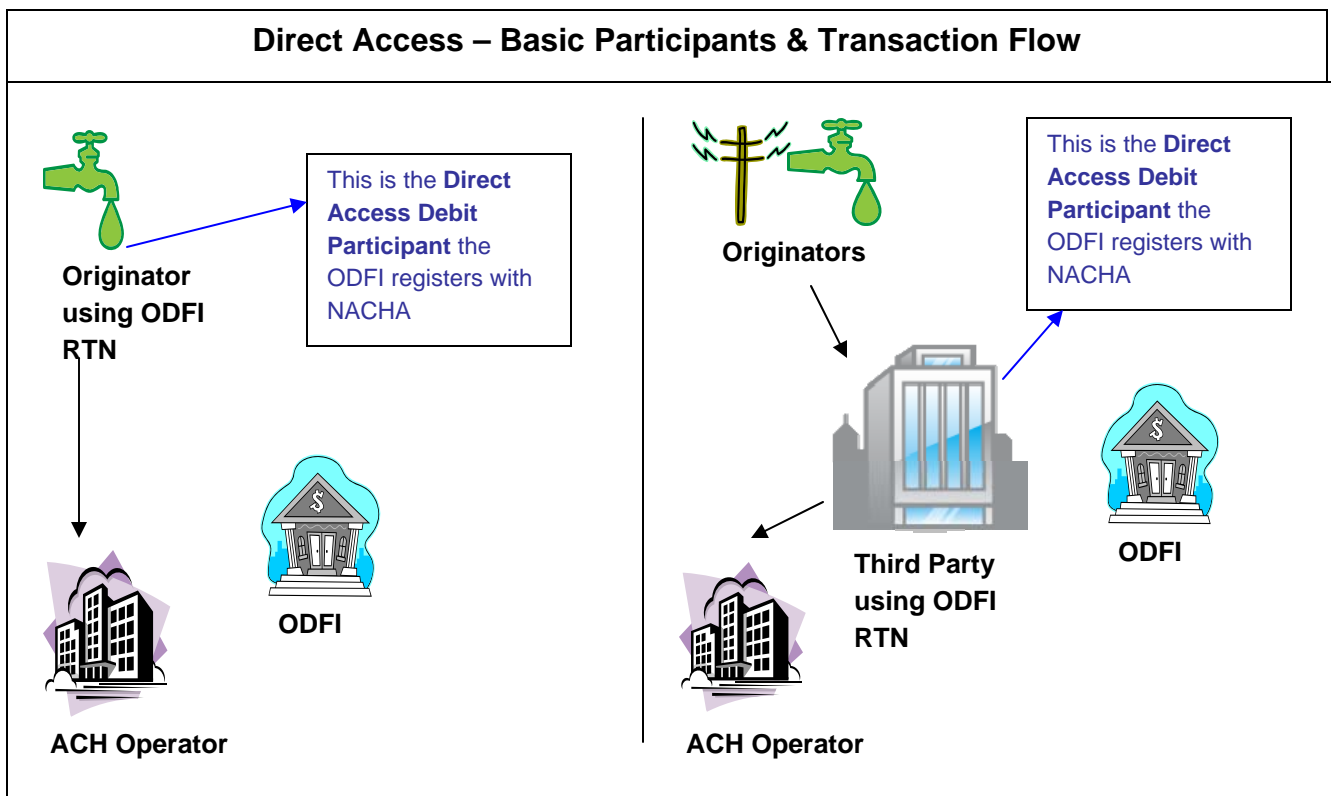
Where do financial institutions go for more information?

Direct Access forms and more information on the registration can be found at:
<http://www.nacha.org/c/DirectAccessRegistration.cfm>

Additionally, NACHA recently issued an ACH Operations Bulletin, *Direct Access Registration Requirement for Originating Depository Financial Institutions*. The Bulletin can be found at:
<http://www.nacha.org/c/OpsBulletins.cfm>

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 ODFI's 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: 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 an ODFI that transmits files using another Participating DFI's routing number and settlement account.



Risk Management and Assessment Rule Effective June 18, 2010

The Risk Management and Assessment rule requires that all Participating DFIs conduct a risk assessment of their ACH activities and implement risk management programs based on the results of such assessments, in accordance with the requirements of their regulator(s). Generally, regulators stress the importance of assessing the nature of risks associated with ACH activity, performing appropriate know-your-customer due diligence, establishing controls for Originators, third parties and Direct Access relationships and having adequate management, information and reporting systems to monitor and mitigate risk.

The rule, effective June 18, 2010, impacts all Participating DFIs by the requirement to perform a risk assessment. The impact is lessened by the number of DFIs that already conduct a risk assessment.

ODFIs are also impacted by the requirements to conduct additional risk management practices prior to originating ACH entries and cover specific topics in their Originator and Third-Party Sender agreements. The impact depends on the nature and complexity of each ODFI's ACH activity. ODFIs that do not conduct similar risk management practices or those that need to revise their Originator agreements will be the most affected. Requirements to modify Originator and Third-Party Sender agreements apply to those entered into or renewed after June 18, 2010. There is no requirement to modify agreements in place before June 18, 2010.

This rule provision outlines certain rights that ODFIs have related to their Originators and Third-Party Senders including:

- the right to terminate or suspend an Originator, or any Originator of a Third-Party Sender, or the Third-Party Sender for breach of the *Rules*; and
- the right to audit an Originator's, or Third-Party Sender's and its Originators', compliance with their agreement with the ODFI and the *Rules*.

ODFIs are required to address their rights to terminate or suspend, audit, and place restrictions on ACH origination activity within any new or renewed agreement with their Originator or Third-Party Sender. There are no new restrictions on origination activity prescribed in this rule provision. Each ODFI is required to address its internally-developed restrictions on origination, if any, within its Originator and Third-Party Sender agreements so as to highlight the importance, and improve the enforcement, of such restrictions.

ODFIs are required to perform a more comprehensive set of risk management practices in addition to the current *Rules* on exposure limits. These requirements include performing due diligence with respect to Originators and Third-Party Senders sufficient to form a belief that the party has the capacity to perform its obligation in conformance with the *Rules*, assessing the nature of the Originator's or Third-Party Sender's ACH activity and the risks it presents, establishing procedures to monitor the Originator's or Third-Party Sender's origination volume and return activity, relative to its exposure limit, across multiple settlement dates and enforce the exposure limit, and establishing procedures to enforce restrictions on the types of ACH transactions that may be originated.

Current requirements for ODFI risk management are limited in the *NACHA Operating Rules (Rules)* to establishing, reviewing, and modifying exposure limits for an Originator's activities. New requirements reflect ACH industry best practices, send a strong message to the industry on the importance of risk management, ensure that all ODFIs perform know-your-customer due diligence and establish procedures, systems and controls to manage the risks of their Originator's and Third-Party Sender's ACH activities.

Examples of recent risk management requirements and guidance by regulators include:

- *FFIEC Retail Payment Systems IT Examination Handbook, February 2010*
(<http://www.ffiec.gov/ffiecinfobase/booklets/Retail/retail.pdf>)
- *OCC Bulletin 2006-39, Automated Clearing House Activities, September 1, 2006*
(<http://www.occ.treas.gov/ftp/bulletin/2006-29.pdf>)
- *FFIEC's BSA/AML Examination Manual, 2007 edition*
(http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2007.pdf) (pages 199 through 205)
- *OCC Bulletin 2008-12, Payment Processors, April 24, 2008*
(<http://www.occ.treas.gov/ftp/bulletin/2008-12.html>)
- *FDIC Financial Institution Letter 127-2008, Payment Processor Relationships, November 7, 2008*
(<http://www.fdic.gov/news/news/financial/2008/fil08127.html>)
- *FFIEC Guidance on Risk Management of Remote Deposit Capture, January 14, 2009*
(http://www.ffiec.gov/pdf/pr011409_rde_guidance.pdf)

Corporate Account Takeover

These Cyber Schemes Can Lead to Fraudulent Transactions

The following article is taken from the ACH Operations Bulletin issued December 2, 2009. For the complete Bulletin, go to: 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 login 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 details of the business, including account activity and patterns, 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 money mules withdraw the entire balances shortly after receiving the money, and then send the funds overseas via over-the-counter wire transfer or other 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 5)

Corporate Account Takeover (Cont'd)

- Small businesses bank with a wide variety of financial institutions with varying degrees of IT resources and sophistication. Some financial institutions may not offer or require services that would defend against corporate account takeover.

WHAT CAN A FINANCIAL INSTITUTION DO?

Financial institutions and business customers have distinct responsibilities to help address the security of online access to business accounts. Each can take steps to protect business 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.

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.

- 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, or is not connected to an internal network.
- Monitor and reconcile accounts daily. Business clients need to reconcile their bank accounts on a daily basis, so that fraudulent activity can be recognized before it is too late to take action.
- Utilize routine and “red-flag” reporting (i.e., alerts about unusual activity) for transaction activity.

ACH OPERATOR SERVICES

Financial institutions should consider fraud detection and risk management services offered by the ACH Operators. For example, a threshold or a cap on ACH credit origination could alert a financial 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:

- 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.

Risk Management Advisory Group

Initiatives for 2010

Data Security

RMAG is collaborating with the Internet Council to develop a business case for rules-based data security requirements for the ACH Network. This holistic approach would be developed based on the ACH transaction lifecycle and would be a well-defined security program/framework that addresses comprehensive policies, procedures, rules, guidelines, and enforcement.

ACH Benchmarking

NACHA staff and RMAG are working in collaboration with the American Bankers Association on a benchmarking effort to develop a means to collect and report on attempted and actual ACH losses. This will allow for the most accurate data to be available in the industry and for trend analysis over time. This collaboration is focusing on: (1) input on the ACH section of the ABA's biannual Deposit Account Fraud Survey, and (2) the development and piloting of a financial institution peer group study.

Terminated Originator Database

The Terminated Originator Database would be a risk management tool based on information shared between ODFIs in a secure environment. The database would be a collection of certain information on terminated Originators and Third-Party Senders that would be provided by contributing financial institutions. ODFIs would access the database to have a more complete risk profile when determining whether or not to begin origination for an Originator or Third-Party Sender.

Direct Access Credit Origination

RMAG will develop and disseminate best practices to ACH participants on risk management related to Direct Access credit origination. Direct Access credit origination typically involves payroll and disbursement entries. (See related article on *Direct Access Debit Participant Relationships and Direct Access Registration* on Page 1.)

Network Enforcement Rule Evaluation

After two years of statistics and lessons learned from the Network Enforcement rule, RMAG will analyze the effectiveness of the rule and determine if modifications should be made to increase its efficiency.

Corporate Account Takeover

Corporate Account Takeover is a specific type of cyber crime that targets small- to medium-sized business customers of financial institutions in which the business' online credentials are compromised. RMAG is developing comprehensive communications and educational materials for business customers, ODFIs, and Third-Party Service Providers in collaboration with NACHA's Communications & Marketing Advisory Group. (See related article on *Corporate Account Takeover* on Page 4.)

Remotely Created Checks

RMAG studied RCCs and non-check e-checks to analyze risks in comparison to ACH transactions. RMAG identified opportunities that could make ACH transactions a payment method of choice over RCCs, such as faster settlement for specific ACH transactions, recurring TEL transactions, and notice equals authorization for the collection of NSF fees.

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.



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

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 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



Check Out These Risk and Compliance Concurrent Sessions at PAYMENTS 2010

Risk Through the Eyes of a BSA Officer

Monday, 8:00 a.m. - 9:00 a.m.

What types of BSA risks exist and how do institutions deal with those risks? Speakers explore risk mitigation from the perspective of the BSA profession and discuss the experiences of institutions with significant international ACH activity. Learn how they manage the BSA/AML risks of these transactions.

Third-Party Risk: Keeping You & Your Bank Out of Trouble

Monday, 11:15 a.m. - 12:15 p.m.

Speakers examine third party risk in the ACH Network through a series of real-world case studies from NACHA's Risk Management Advisory Group (RMAG). For each case study, speakers examine what went wrong and why, and more importantly, what they missed during new customer implementation, ongoing operations, or the period when banks were trying to close down their Third-Party Processors.

Business Continuity - Are You Ready for Anything?

Monday, 1:30 p.m. - 2:30 p.m.

Does your business continuity plan need retooling? Effective business continuity planning is about being ready when, not if, disaster strikes. Topics include the general activities of local banks, payments systems, and businesses in the aftermath of these disasters as they worked through the recovery process in their attempt to return to normal activity.

NACHA's Risk Management Strategy Update

Monday, 1:30 p.m. - 2:30 p.m.

NACHA's Risk Management Advisory Group (RMAG) identifies sources of risk in the ACH Network and develops efficient, targeted approaches to risk mitigation. Speakers review what's on the horizon for RMAG and the risk environment and discuss critical initiatives designed to ensure high-quality ACH transactions and reduce risk for all Network participants.

Fraud & Security: The Next Generation

Monday, 4:30 p.m. - 5:30 p.m.

Two of the largest fraud solution providers meet to discuss fraud as it exists today. Speakers explore the challenges providers and financial institutions face and examine trends and analysis concerning threats to business practices.

Realizing End-to-End Encryption & Data Level Security in the Payments Industry

Monday, 4:30 p.m. - 5:30 p.m.

Payment card data is a valuable target for fraudsters. The speaker reviews the challenges and opportunities facing the payments industry to secure sensitive card data through end-to-end encryption, card authentication technologies, and post-processing tokenization, as well as the prospect of applying these data security technologies to reduce and/or limit the scope and cost of PCI.

The Tangled Web: Attacks on Business Credentials

Tuesday, 8:00 a.m. - 9:15 a.m.

Online fraud involving the compromise of business' online banking credentials is increasing. Through a series of case studies, attendees hear how malware, phishing, and social engineering are affecting financial institutions and account holders. Learn how to protect your institution and business customers by understanding the threats and what actions you and your business customers should take to aggressively thwart them.

IAT Fraud Risk & Compliance Challenges

Tuesday, 8:00 a.m. - 9:15 a.m.

Specific aspects of IAT (such as the variations in reversal and return policies by country) combined with the generally higher risk level associated with cross-border money transfers present significant fraud risk threats for financial institutions originating and receiving IATs. The operational challenges presented by interdiction and resolution of a higher volume of both sanctions and fraud issues are potentially significant.

Legal Issues for Emerging Payment Products

Tuesday, 8:00 a.m. - 9:15 a.m.

Speakers focus on issues for new micropayment mechanisms; the status of key issues for growth in the mobile payment segment, including licensing issues, AML issues, the application of Regulation E, mechanisms for eSign compliance and use of multi-factor authentication; and the implications of the CARD Act for the viability of prepaid products.

(Cont'd on Page 9)

(Cont'd from Page 8)

Collaboration to Address Payments Fraud

Tuesday, 10:00 a.m. - 11:15 a.m.

Speakers engage in a cross-perspective discussion on the roles of the payments industry, law enforcement, regulators, and others, and examine how groups can best share information, police bad actors, and otherwise collaborate to improve the integrity of retail payments systems for the good of all.

PayPal & GMAC - Fighting Fraudsters: Protecting Your Company from Fraud

Tuesday, 10:00 a.m. - 11:15 a.m.

Speakers examine the latest trends in fraud and how companies can protect themselves from such activities as they review the complete range of fraud prevention issues, from on-boarding clients, authenticating identities, identifying trusted parties, validation of accounts, ACH positive pay, Universal Payment Identification Codes (UPIC's), Office of Foreign Assets Control (OFAC), debit blocking, and pseudo-accounts.

Using Link Analysis to Identify Crime Rings & Mitigate Losses

Tuesday, 1:30 p.m. - 2:30 p.m.

Professional and sophisticated fraudsters usually work within crime rings and are difficult to identify. Link analysis is the next generation in fraud prevention. For the past year, Early Warning has been working with Compass Bank to perform link analysis related to data in the National Shared Database. The two organizations present the results of their collaboration and provide an update on their progress.

Third-Party Senders - Risks & Best Practices

Tuesday, 1:30 p.m. - 2:30 p.m.

Speakers provide an overview of the risks Third-Party Senders introduce into the ACH Network. Attendees learn from the regulators about examination findings and deficiencies noted for ODFIs that had not appropriately mitigated the risk resulting from Third-Party Sender activity. Presenters highlight best practices that one large bank employs to mitigate the risk of using Third-Party Senders, including due diligence, agreements, operating and monitoring criteria.

What's The Best Way to Steal a Company's Online Banking Credentials?

Tuesday, 3:15 p.m. - 4:15 p.m.

Fraudsters have become creative and sophisticated in figuring out how to steal business customers' online banking credentials and engage in fraudulent activity. This presentation features a detailed visual description of how online criminals target business' online banking software and details the roles of Man-In-The-Browser (MITB) Trojans and mule networks.

Fraud Prevention & Risk Management: How to Pre-Determine False Checks and Crack Down on Fraudsters

Tuesday, 4:30 p.m. - 5:30 p.m.

The industry understands well the merchant and consumer benefits of allowing check payments. Speakers address today's best-in-class fraud prevention tools and explain how authorization systems validate IDs, issue risk management decisions and settle transactions if approved.

Receipt Fraud: Reducing your Losses Across Payment Channels

Tuesday, 4:30 p.m. - 5:30 p.m.

As the "Fraud Business" continues to evolve there are significant changes to the types of fraud being committed. Learn how two companies work together to spot and reduce exposure to receipt fraud as it becomes a cross-channel risk for all.

Lessons from the Front: Payments in the Credit Crossfire

Wednesday, 8:30 a.m. - 9:30 a.m.

Leading economists have called the recent recession affecting the domestic and global economies over the past two years, the most serious financial crisis since the Great Depression. It encompasses failures in the consumer, financial, industrial, and business sectors of the economy. Speakers in this session focus on the effects of the crisis on payments, payment methods, and working capital.

Growing Risks & Challenges of e-Payments Enrollments

Wednesday, 9:45 a.m. - 10:45 a.m.

Speakers in this session share information about the risks, challenges, opportunities, and benefits of e-payments; how critical first filters in the e-payments; processes to help reduce fraud and losses, while increasing revenue and enhancing customer service; and details how contributing Account Owner Elements data and Account Status data to the National Shared Database delivers enterprise-wide benefits.

A Changing Payments Landscape Requires Innovative Fraud Management

Wednesday, 11:00 a.m. - 12:00 p.m.

Radical change in bank payment systems has led to increased productivity, new business development opportunities, and more fraud. Speakers examine fundamentally new approaches to detecting and preventing fraud in payment systems and examine how loss prevention professionals can prepare for the continued evolution of the payments system.