ACH Fraud Prevention in the Electronic World

Presented by:
Debbie Smart, CTP, NCP
Senior Business Consultant
Q2

What We Will Cover

- Introductions and Overview
- ACH Volume Growth
- Types of ACH Risk
- Managing Credit Risk
- Managing Operational Risk
- Managing Fraud Risk
- Conclusion and Q & A

ACH Volumes by Payment Type

Overall ACH Volume More Than 25.5 Billion in 2016

2016 ACH Network Transactions (does not include on-us volumes)			
	2016	2015	% change
ARC	1,345,599,186	1,466,889,179	-8.27%
BOC	125,073,732	146,477,682	-14.61%
CCD Debits	1,000,736,647	950,361,077	5.30%
CCD Credits	1,973,146,280	1,878,153,317	5.06%
CIE	161,778,517	162,295,206	-0.32%
CTX	111,045,469	104,750,968	6.01%
IAT	83,020,829	73,660,089	12.71%
POP	265,493,836	310,281,327	-14.43%
PPD Debits	3,724,164,948	3,564,402,091	4.48%
PPD Credits	6,115,487,264	5,819,349,897	5.09%
RCK	2,661,108	3,095,278	-14.03%
TEL	505,384,533	465,400,576	8.59%
WEB Debits	4,579,477,314	4,065,441,536	12.64%
WEB Credits	78,963,243	57,028,566	38.46%
Other	256,714,211	245,516,748	4.56%
Total Network	20,328,747,117	19,313,103,537	5.26%

ACH Risk Overview

ACH Risk Overview

- Five Types of ACH Risk:
- Systemic - The risk that the inability of an ACH network participant to settle its commitments results in the inability of other participants to settle their obligations (the participating DFI has no control over management of this type of risk).
- Operational - The risk of loss related to errors or omissions which may result in delayed, duplicated or otherwise erroneous payments. Operational risk may result from human or equipment (hardware, software, telecommunications) failure.
- Fraud - The risk that a payment transaction is initiated or altered in an attempt to misdirect or misappropriate funds. Fraud risk includes the introduction of false transactions or the alteration of otherwise valid transactions.
- Reputational - The risk that arises from adverse publicity related to a negative financial event, resulting in a loss of business. Sources of reputational risk include word of mouth, media coverage and news publications.
- Credit - The risk that one party to an ACH transaction will be unable to provide the necessary funds for payment settlement.

Q2

ACH Credit Risk

Credit Risk

- Risk that a party to a transaction cannot provide the necessary funds in order for settlement to take place

Q2

ACH Credit Origination – 2 day example

Monday	Tuesday	Wednesday
•ACH credit file sent from Company to Bank •Entries are effective on Day 3 (Wednesday) •Bank processes file and delivers transactions to ACH Processor	•ACH credits are delivered to RDFIs by the ACH Processor	•Bank's account is charged by the ACH Operator •Company declares bankruptcy

ODFI Exposure

Q2

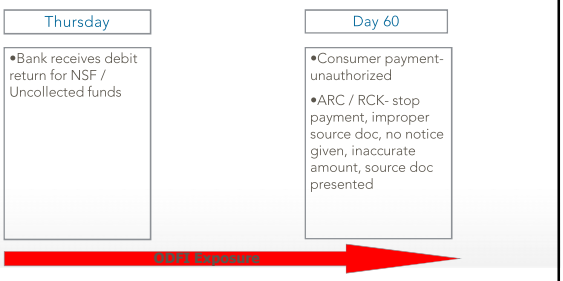
ACH Debit Origination

Monday	Tuesday	Wednesday
•ACH debit file sent from Company to Bank •Entries are effective on Day 2 (Tues) •Bank processes file and delivers items ACH Processor	•ACH debits are delivered to RDFIs by the ACH Processor •Bank credits Company for amount of debit file •RDFIs reject debits for NSF	•RDFIs return debits •Company declares bankruptcy

ODFI Exposure

Q2

ACH Debit Origination



Q2

Managing ACH Credit Risk

Underwriting

ODFI's should:

- Know your customer!
- Treat all ACH origination customers as unsecured borrowers;
- As such, subject them to credit review and approval process;
- Establish acceptable credit limit;
- Monitor creditworthiness of customers on an on-going basis.

Q2

Pre-funding as an Alternative

- Originating customer "pays in advance"
- When ACH files are submitted for processing, the customer's account is debited prior to the transactions being released into the network
- Eliminates need for the ACH credit review process
- Consider for customers who are new to the bank or don't pass credit standards for traditional origination services

Q2

Additional Sound Practices

- Set limits reflective of the customer's credit limit
  - Receive alerts when limits are met/exceeded
  - Review and decision exception items
- Set limits reflective of the customer's usual activity
  - Receive alerts when anomalies occur
  - Review and decision exception items
- Limit SEC codes to what the customer will be originating and/or is allowed to originate

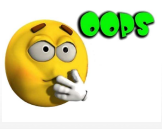
Q2

ACH Operational Risk

Grow Beyond. www.q2ebanking.com

ACH Operational Risk

- The risk of loss related to errors or omissions which may result in delayed, duplicated or otherwise erroneous payments.
- Operational risk may result from human or equipment (hardware, software, telecommunications) failure.



Q2

ACH Operational Risk

Examples of Operational Risk

- Slip of a finger on a keyboard
- Failure of a piece of hardware or software
- Communications protocol problems
- Narrow decision windows
- Inadequate information
- Being short-staffed
- Breaches in internal controls

….to name a few

Q2

Managing Operational Risk

Sound Practices for Mitigating and Managing Operational Risk

- Quickly identify and act upon anomalies at the customer level.
  - Customer level control enables ODFIs to monitor a specific batch within an ACH file without delaying the processing of the rest of the file.
- Have an efficient notification system in the event of credit or debit cap breaches, or other issues that may impact the decision whether to release or reject an ACH batch.
- In the event of a hardware, software or power failure, maintain access to ACH activity. Services that use Web-based technology afford access to authorized/credentialed personnel from virtually any computer terminal with an Internet connection.

Q2

ACH Fraud Risk

Grow Beyond. www.q2ebanking.com

ACH Fraud Risk

- The risk that a payment transaction is initiated or altered in an attempt to misdirect or misappropriate funds. Fraud risk includes the introduction of false transactions or the alteration of otherwise valid transactions.

Q2

ACH Fraud Risk

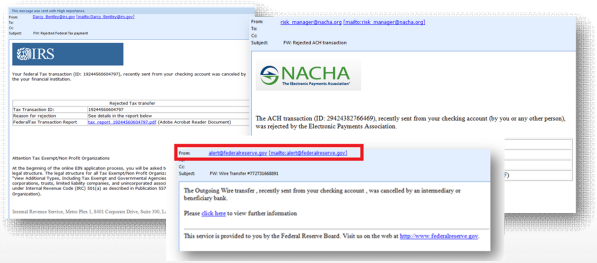
Examples of Fraud Risk

- Account Takeover:
  - a type of identity theft in which a criminal steals a business's (or individual's) valid online banking credentials and then uses those credentials to initiate funds transfers out of the account
- Business Email Compromise and Vendor Impersonation Fraud (phishing)
  - one method of gaining valid online banking credentials

Q2

Phishing Examples

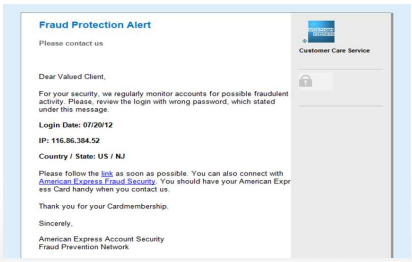
Impersonating Authority



Q2

Phishing Examples

Impersonating Vendors



Fraud Protection Alert

Please contact us

Customer Care Service

Dear Valued Client,

For your security, we regularly monitor accounts for possible fraudulent activity. Please, review the login with wrong password, which stated under this message.

Login Date: 07/20/12

IP: 116.86.384.52

Country / State: US / NJ

Please follow the link as soon as possible. You can also connect with American Express Fraud Security. You should have your American Express Card handy when you contact us.

Thank you for your Cardmembership.

Sincerely,

American Express Account Security
Fraud Prevention Network

Q2

Managing Fraud Risk

Multi-pronged, multi-layerd

- Sound Business Practices for Financial Institutions
- Sound Business Practices for Companies
- Sound Business Practices for Third-Party Service Providers

Q2

Sound Business Practices for Financial Institutions

Sound Practices for Mitigating and Managing Fraud Risk

- Agreements & Minimum Security Procedures
- Dual Control for Payment File Initiation
- Out-of-Band Authentication and Alerts
- Enhancement of Account Security Offerings
- Exploration of Low-Tech Security Options
- Education
- Special Considerations for RDFIs

Q2

Sound Business Practices for Financial Institutions

Sound Practices for Mitigating and Managing Fraud Risk

- Agreements & Minimum Security Procedures should include:
  - Advise implementation of multi-factor and multi-channel authentication for business accounts that are permitted to initiate funds transfers. Multi-factor authentication includes at least two of the following:
    - something the person knows (user ID, PIN, password)
    - something the person has (password-generating token, USB token)
    - something the person owns (biometrics, i.e., fingerprint scan)

Q2

Sound Business Practices for Financial Institutions

Sound Practices for Mitigating and Managing Fraud Risk

- Out-of-Band Authentication and Alerts
  - Use out-of-band alerts to warn an Originator of unusual activity. Triggers may include:
    - New payees: Recipients who have never received a transfer from the Originator before.
    - IP address authentication: A file is initiated from an IP address not previously associated with the Originator.
    - New credential requests: Someone at the financial institution should be evaluating requests for new Originator credentials before issuing and permitting use of the new credentials.
    - Abnormal patterns: time of day, day of week, unusual amounts and transaction counts

Q2

Sound Business Practices for Financial Institutions

Sound Practices for Mitigating and Managing Fraud Risk

- Enhancement of Account Security Offerings
  - Encourage Originators to use value-added services like positive pay, debit blocks, and tokens to enhance Originator's account security.
- Exploration of Low-Tech Security Options
  - Origination calendar: Consider using origination calendars that will alert a financial institution to files that are out of the normal behavior (e.g., different time of day or different amount than is typical) for the client.
  - Prenotification: Consider using prenotification for credit origination when an Originator makes changes to their origination file (e.g., adding new Receivers or account number changes).

Q2

Sound Business Practices for Financial Institutions

Sound Practices for Mitigating and Managing Fraud Risk

- Special Considerations for RDFIs:
  - Educate front-line staff about money mules and what to do if one is suspected or identified.
  - Look for anomalies in deposits.
  - Develop procedures for what to do if a money mule is suspected or identified.

Q2

Sound Business Practices for Companies

Sound Practices for Mitigating and Managing Fraud Risk

- Computer Security:
  - Layered System Security
  - Online Banking Safety
  - Education
  - Websites
  - User Accounts
  - Staying Informed
- Account Security:
  - Dual Control
  - Reconcilement
  - Account Services
  - Reporting of Suspicious Activity
  - Credentials

Q2

Sound Business Practices for Third-Party Service Providers

Sound Practices for Mitigating and Managing Fraud Risk

- Third-Party Senders Performing Services on Behalf of an Originator:
  - Educate Originators
  - Dual Control for Payment Initiation
  - Agreements and Minimum Security Procedures
  - Exposure Limits
  - Enhancement of Account Security Offerings
- Third-Party Service Providers Performing Services on Behalf of an ODFI or an RDFI
  - Follow Sound Practices for Financial Institutions

Q2

Summary

- ACH risk must be understood and monitored
- Many tools/sound practices help mitigate more than one type of risk
- Education – both employees and customers – is critical
- With the right tools in place, you can feel confident you are providing the right services to your customers and properly managing your exposure
- Remember – There is risk inherent in all aspects of banking – lending, merchant services, deposit accounts – understanding, managing and mitigating risk – it's what we do!
- Great resources for more information:
  - nacha.org
  - frbservices.org

Q2

The End ☺

Questions??

Debbie Smart, CTP, NCP
Phone: **702-540-3061**
Email: **Debbie.smart@q2ebanking.com**

Grow Beyond. www.q2ebanking.com