Alternatives for Managing Commercial Payments Risk

FDIC Symposium
Arlington, VA
May 11, 2010

Deborah Shaw
Managing Director, Network Enforcement & Risk Management
NACHA – The Electronic Payments Association

NACHA
The Electronic Payments Association®

NACHA and the ACH Network

- As administrator of the ACH Network, NACHA:
  - creates and maintains the *NACHA Operating Rules*,
  - enforces the *Rules*,
  - proactively develops Network risk policy, and
  - responds to Network risk events

- NACHA implements its risk strategy by:
  - making changes to the *NACHA Operating Rules*,
  - disseminating best practices,
  - identifying industry offerings available to mitigate risk, and
  - developing tools to manage the risk profile of the Network on an ongoing basis

NACHA The Electronic Payments Association®

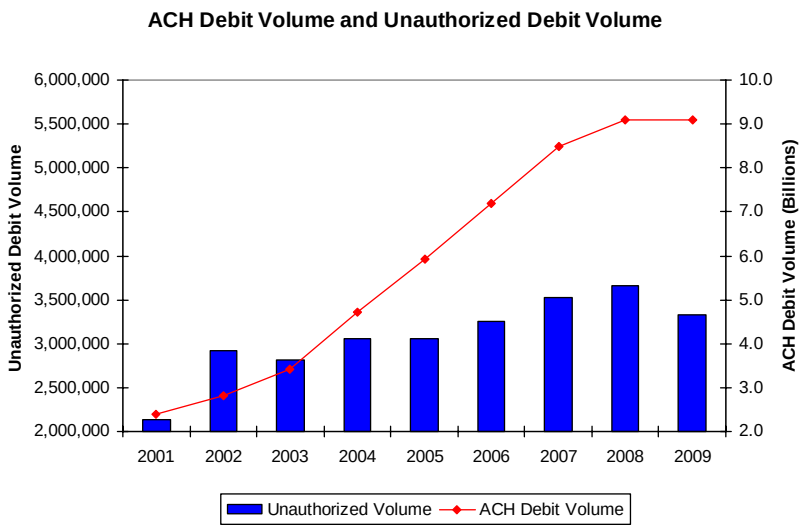
Background

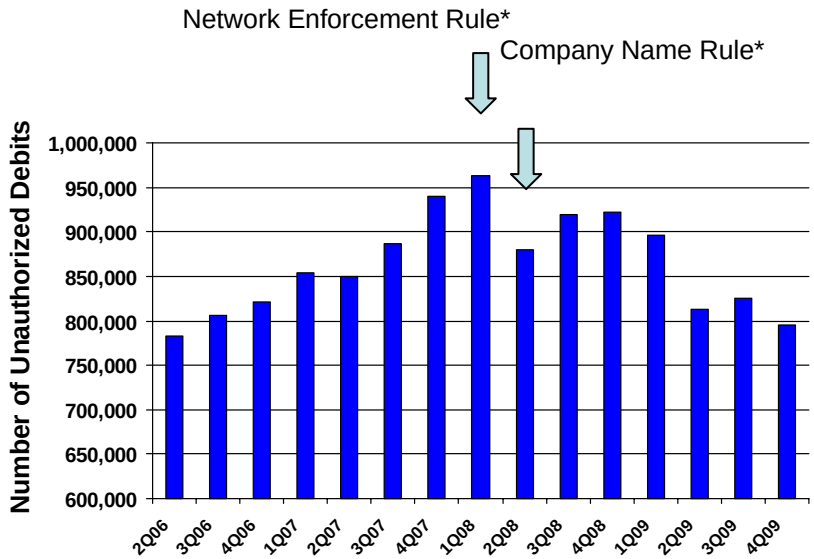
- Types of ACH Applications:
  - Debit transactions
  - Credit transactions
- Return codes are tracked, such as:
  - Unauthorized
  - Invalid account
  - Not sufficient funds
- "Traditional fraud" typically involved debit payments: including telemarketing fraud, credit repair, and membership clubs using ACH debit applications
  - Unauthorized debit return rates as key indicator
- Since 2001, debit unauthorized return rates fell move than 50% from .09% to .04%
- Recently fraud activity targeting businesses has resulted in fraudulent credit payments
  - ACH credits
  - wire transfers

NACHA The Electronic Payments Association®

Risk Mitigation Efforts have been Robust

- ACH Debit Transactions grew 18.1% CAGR, while unauthorized returned debits grew at 5.9% CAGR
- The impact of solid Network-wide *Rules* and risk management efforts shows in the downward trend of the absolute volume of unauthorized debit returns





NACHA The Electronic Payments Association®

What is Corporate Account Takeover?

- A type of identity theft in which cyber-thieves gain control of a business' bank account by stealing the business' valid online banking credentials through malware (among other methods)
  - Corporate account takeover is about compromised identity credentials – it is not about compromises of the wire system or ACH Network
- A computer can become infected with malware which can then spread across the business' entire internal network. This can happen through:
  - infected documents attached to an e-mail
  - a link contained within an e-mail that connects to an infected web site
  - visiting legitimate web sites - especially social networking sites - and clicking on the documents, videos or photos posted there
  - a USB port using a flash drive (that was infected by another computer)
- The cyber-thieves can then initiate funds transfers, by ACH or wire transfer, to the bank accounts of associates within the U.S. ("Money Mules") or directly overseas (with wires)

NACHA The Electronic Payments Association®

FI and Business Partnership to Protect Against Cyber-thieves

- Smaller FIs and small and medium-sized businesses are being targeted because they are perceived by criminals as more likely to have insufficient controls
- The perception is that many small businesses do not practice dual control, do not utilize value-added banking services, and do not monitor and reconcile their accounts on a frequent or daily basis
- Financial institution and business customers have distinct responsibilities to help address the security of online access to accounts

NACHA The Electronic Payments Association®

Recommendations for Originating FIs

- Deploy multi-factor and multi-channel authentication
- Require dual control
- Enable out of band transaction verification
- Provide out of band alerts for unusual activity
- Establish and monitor exposure limits that are related to the customers' activities
- Explore tools offered by vendors to prevent or detect fraud
- Consider the risk management services offered by the ACH Operators
  - e.g., ACH Origination Threshold/Cap
- Educating business customers is essential to risk mitigation strategies

Recommendations for Receiving FIs: How to Spot a Money Mule

- According to the FDIC, money mule activity is essentially electronic money laundering addressed by the Bank Secrecy Act and AML regulations
- How to Spot a Money Mule
  - A financial institution can look for a pattern of activity that is consistent with corporate account takeover:
    - A new account opened by a customer with a small deposit, followed shortly by one or more large deposits by ACH credit or wire transfer
    - An existing account with a sudden increase in the number and dollar amounts of deposits by ACH credit or wire transfer
    - A new or existing accountholder that withdraws a large amount of cash shortly after a large deposit (often 5-10% less than the deposit)
- In many cases, the dollar amounts of deposits and withdrawals are around $9000

NACHA The Electronic Payments Association®

Recommendations for Businesses

- Initiate ACH and wire transfer payments under dual control. For example:
  - One person authorizes the creation of the payment file
  - A second person authorizes the release of the file
- 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: use a dedicated computer to conduct online banking and payments activity
- Monitor and reconcile accounts daily

NACHA The Electronic Payments Association®

Recommendations for Businesses

- Install commercial anti-virus and desktop firewall software on all computer systems
- Ensure anti-virus and security software is up to date
- Utilize routine and “red-flag” reporting for transaction activity
- Never access bank accounts at Internet cafes, or from public wi-fi hotspots (airports, etc)
- Additional resources for businesses:
  - BBB outreach to small businesses: Data Security Made Simple

NACHA Communications and Collaboration

- Partnerships are the solution to combating fraud
  - All parties have a role
  - Communicate broadly and accurately
- NACHA communications
  - 2007 and again in 2009: NACHA Risk Alerts and Members' Memos about keylogging and "Corporate Account Takeover"
  - Referenced 2005 FFIEC Guidance – Authentication in an Internet Banking Environment
- Collaboration with FS-ISAC and FBI on FI Alert
  - Communicated issues and best practices to financial Institutions and industry
- Drafted new section for Better Business Bureau Data Security publication for small businesses – "Data Security Made Simple"
- Held Teleseminars on risk / keylogging issues to educate FIs and Network participants
  - NACHA sponsored / ABA sponsored
- Risk Management Vendor Showcase – FFIEC Regulatory Panel
- Cyber Attack Against Payment Processes – in cooperation with FS-ISAC
  - February 2010 – 3 day simulation of cyber attacks
  - Raise awareness / make recommendations

NACHA The Electronic Payments Association®