Security and Risk:
NACHA and the ACH Network

Payment Innovations in the Wake of the Financial Crisis
Federal Reserve Bank of Chicago
May 21, 2010

Jan Estep
President and CEO
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

Background

- Types of ACH Applications:
  - Debit transactions
  - Credit transactions

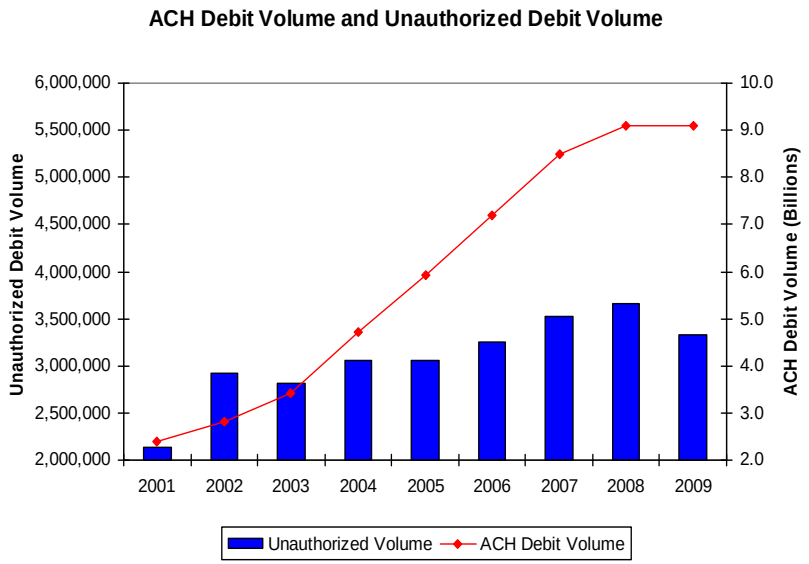
- Return codes are tracked, such as:
  - Unauthorized
  - Invalid account
  - Not sufficient funds

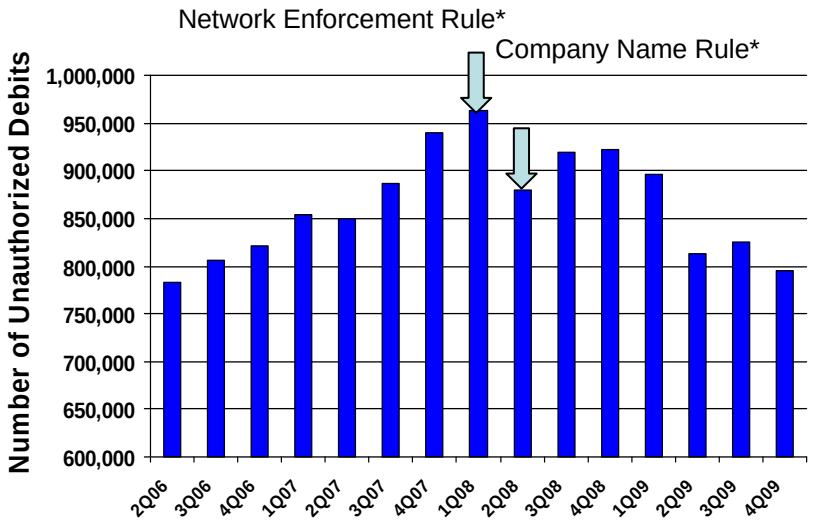
- “Traditional fraud” includes telemarketing fraud, credit repair, and membership clubs using ACH debit applications
  - Unauthorized debit return rates as key indicator

- Since 2001, debit unauthorized return rates fell from .09% to .04%.

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®

Perspective on Risk and Losses *

- Of the victims of attempted ACH fraud, only 11% also suffered a financial loss
  - Didn't follow best practices:
    - no ACH positive pay / not timely return / online system not well protected
  - Smaller organizations were more likely to have suffered a financial loss from ACH fraud (18%) - compared to 9% of organizations with annual revenues > $1B
- Nearly 80% of organizations have fewer than 10 ACH fraud attempts per year

Payment Method	% subject to actual or attempted fraud	% with increased incidents	Payment method most responsible for losses
Checks	90%	89%	64%
ACH Debits	25%	11%	5%
Consumer Cards	20%	13%	20%
Corporate Cards	17%	8%	8%
ACH Credits	7%	3%	1%
Wire Transfers	3%	2%	2%

* Source: AFP 2010 Payments Fraud and Control Study

NACHA The Electronic Payments Association®

Types of Fraud – Paradigm shift?

- More activity lately regarding unauthorized funds transfers from DDAs – mainly credit payments (wire and ACH)
  - Corporate account takeover of online banking tools (credentials compromised)
    - Once the fraudster has access to the account, can do anything the legitimate account holder can do – often including assuming administrative rights

- Because there are no returns, data related to credit transactions that the Originator claims as unauthorized are not collected systematically through the Network
  - Additional shared information is required

- Source of payments fraud resulting in losses in 2009 (all payments, not just ACH) *
    - Outside individual – 87%
    - Organized crime ring – 15%
    - Internal party – 11%
    - Criminal invasion (hacked system, malware) – 4%
    - Other – 4%
    - Stolen laptop – 2%

- Critical to share information – within organizations, across organizations

* Source: AFP 2010 Payments Fraud and Control Study

NACHA The Electronic Payments Association®

Communications and Collaboration

- Communicate broadly and accurately
  - 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®

Approach to Fraud and Risk Mitigation

"Organizations continue to increase their use of controls that protect against ACH fraud." (AFP 2010 Fraud Study)*

1. Debit blocks (75%)*
2. Debit filters (58%)*
3. ACH Positive Pay (21%)*
4. UPIC for credits (5%)*
5. Separate accounts, separate PCs
6. Dual controls
7. Trusteer: Rapport

1. Daily account monitoring and alerts
2. Laru: ACH Vision
3. Fiserv: ACHeck for FraudLink On-Us, and Fraud Risk Manager
4. Operators – reporting of many types

1. Communicate rapidly
2. Rely upon specific contractual obligations
3. Reinforce proper utilization of available tools
4. Laru: ACH Clarity

Note: Prevention, Detection, Resolution Model – Trademark of Javelin Strategy & Research

NACHA The Electronic Payments Association®

Traditional, plus New Tools are Available

- **Prevention** – beyond education – part of layered approach:
  - "Trusteer: Rapport" – to protect online banking identity theft and fraud
    - Combination of access control, encryption and verification tools
    - Locks down customer's browser against malware-based phishing, man-in-the-browser and man-in-the middle – zero-day vulnerabilities

- **Detection:**
  - "Laru: ACH Vision" – gate keeping with customizable business rules
    - Puts the FI in control by putting a hold on files – patterns at individual level
  - "Fiserv: ACHeck for FraudLink On-Us" – creates intelligence across channels
    - Rules apply to ACH, as well as check
  - "Fiserv: Fraud Risk Manager" – customizable fraud detection scenarios
    - Supports ACH originator monitoring – suspends files while client alerts are generated, with seamless next steps

- **Resolution:**
  - "Laru: ACH Clarity" – reporting for limits, rules monitoring, risk assessment
    - Unique modules for RDFI and ODFI – clarifies trends and developing issues

NACHA The Electronic Payments Association®

Move to and Use Electronic Payments and Tools

- "The survey results suggest that perhaps the single best way for organizations to protect themselves against payments fraud is to move away as quickly as possible from the use of checks for payment."

- "While ACH and card fraud is not insignificant, the data...makes it abundantly clear that issuing checks represents the greatest vulnerability to payments fraud for organizations."

- "Organizations large and small should be pushing hard and working with their banks, vendors and other suppliers, to eliminate this vulnerability by moving transactions to ACH and card payments."

* Source: AFP 2010 Payments Fraud and Control Study

NACHA The Electronic Payments Association®