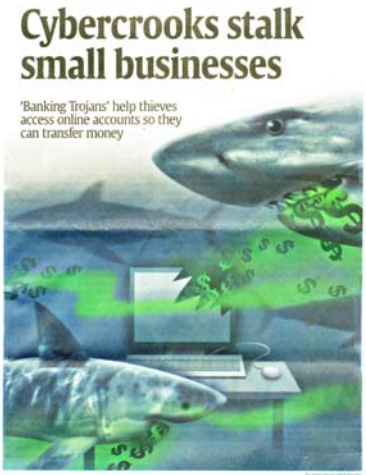
Corporate Account Takeover

American Bankers Association/NACHA
Telephone Briefing
March 23, 2010

Jane Larimer
EVP ACH Network Administration
NACHA – The Electronic Payments Association

NACHA
The Electronic Payments Association®

USA Today Article: December 31, 2009



NACHA
The Electronic Payments Association®

USA Today Article: December 31, 2009

- "Any organization that cannot survive a sudden 5 or 6 figure loss should consider shunning Internet banking altogether," says Amrit Williams of security firm BigFix. "Online is a very dangerous place for any small organization to be right now."

NACHA The Electronic Payments Association

Introduction

- Corporate account takeover is about compromised identity credentials – it is not about compromises of the wire system or ACH Network itself
- Smaller FIs and small and mid-sized businesses are being targeted because they are perceived by criminals as more likely to have insufficient controls
- Reputation risk is growing. There are some perceptions that:
  - Online banking is not safe
  - The wire and ACH Networks are vulnerable
- Educating business customers is essential to risk mitigation strategies

NACHA The Electronic Payments Association

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)
- 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 websites - 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®

USA Today Article: December 31, 2009

- "The victims are mostly small to midsize organizations using online bank accounts supplied by local community banks and credit unions, FBI analysis shows."
- "In a race to win more online business customers, many banks offer high limits on ACH and wire transfers, even though their systems lack modern technologies for detecting fraud."

» Terry Austin, CEO of Guardian Analytics

NACHA The Electronic Payments Association®

Why are Cyber-thieves Targeting Small Businesses and Organizations?

- 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);
- 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 practice dual control, do not utilize value-added banking services, and do not monitor and reconcile their accounts on a frequent or daily basis;
- 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 help defend against corporate account takeover

NACHA The Electronic Payments Association®

What Can an ODFI Do?

- FIs and business customers each have distinct responsibilities to help address the security of online access to accounts
- The top things FIs can do are:
  - 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
  - Educate their business customers on prevention, detection and reporting measures
- FIs should also consider the risk management services offered by their ACH Operators
  - e.g., ACH Origination Threshold/Cap

NACHA The Electronic Payments Association®

Krebs on Security Blog March 16, 2010

- "The banks could do a better job educating customers about the risks they face with banking online, but the business victim ("Eskola") allowed that business owners also need to take their share of responsibility."
- "The banks need to raise this issue front of mind for small businesses, but the guy who runs that small business really needs to step up and be responsible for his end, too," Eskola said.

NACHA The Electronic Payments Association®

What Can a Business Do?

- 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®

What Can a Business Do?

- 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 The Electronic Payments Association 11

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
- An FI 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 12

Additional Resources for FIs

- FS-ISAC/FBI/NACHA White Alert: Account Hijacking of Corporate Customers – Recommendations for Customer Education
- NACHA ACH Operations Bulletin: Corporate Account Takeovers Can Lead to Fraudulent Transactions

Questions?