

# Announcing the FS-ISAC Account Takeover Task Force

**May 11, 2010**



Sharing Critical, Specific, Meaningful, Accurate, Reliable and Timely Information

# Account Takeover Fraud

- Significant increase in account takeover frauds
  - Exploitation of valid online banking credentials effecting small and medium sized businesses
- Activity traced to criminal organizations using sophisticated techniques
  - Phishing / Spear Phishing
  - Drive-by downloads
  - Search Engine Optimization Poisoning
  - Man-in-the-Browser / Man-in-the-Middle Attacks
- Millions of user systems infected with malware such as Zeus Trojan Keylogger
- Results in significant account takeover fraud
  - Millions of dollars in fraud losses
  - Strained business relationships and litigation



# Account Takeover Task Force

- FS-ISAC is taking a proactive lead to address account takeover fraud
- Public / Private Partnership
  - Industry Associations
    - FS-ISAC, ABA, BITS, NACHA, SIFMA, CBA, CUNA, ICBA, MBA, NAFCU + more
  - Government Partners
    - US Treasury, FBI Cyber Division, US Secret Service, FFIEC, Regulatory agencies + more

**FS-ISAC YELLOW:** The contents of this alert are sensitive, and intended only for the recipients and other FS-ISAC members with a need-to-know.



## Corporate Account Takeover Impacts Payment Systems 21 August 2009

*This product was created as part of a joint effort between the Federal Bureau of Investigation, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and NACHA - the Electronic Payments Association, in coordination with the U.S. Department of Treasury.*

### **Background**

Within the last six months, the FBI has seen a significant increase in fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses. In a typical scenario, the attack vector is a "spear phishing" e-mail which contains either an



# Account Takeover Task Force Organization

- Prevention
  - Best practices for fraud prevention and detection for financial institutions
  - Best practices for customer awareness, securing desktops and fraud detection mechanisms
- Detection
  - Enhancing information sharing efforts through identification and dissemination of technical and non-technical threats
- Response
  - Service providers - Developing best practices for responding to fraud
  - Law enforcement - Fraud containment, fraud recovery
  - Strategically address Cyber Crime at the International level

# Account Takeover Task Force

## Membership

- Financial Institutions
- Financial Sector Industry Associations
- Government Participants from Law Enforcement, Regulatory Agencies and other US Government agencies
- Additional participants
  - Send your contact information and short biography or resume to [admin@fsisac.com](mailto:admin@fsisac.com) for consideration

