RADIX
CONSULTING
CORPORATION

the source for your payments needs

Corporate Account Takeover Risk Management

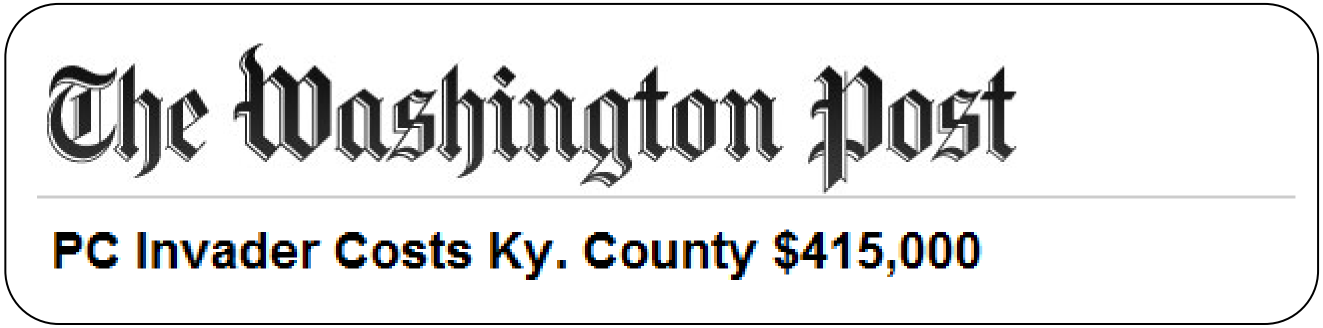
GACHA Solutions 2010 Conference

Rossana Salaris, AAP

Principal

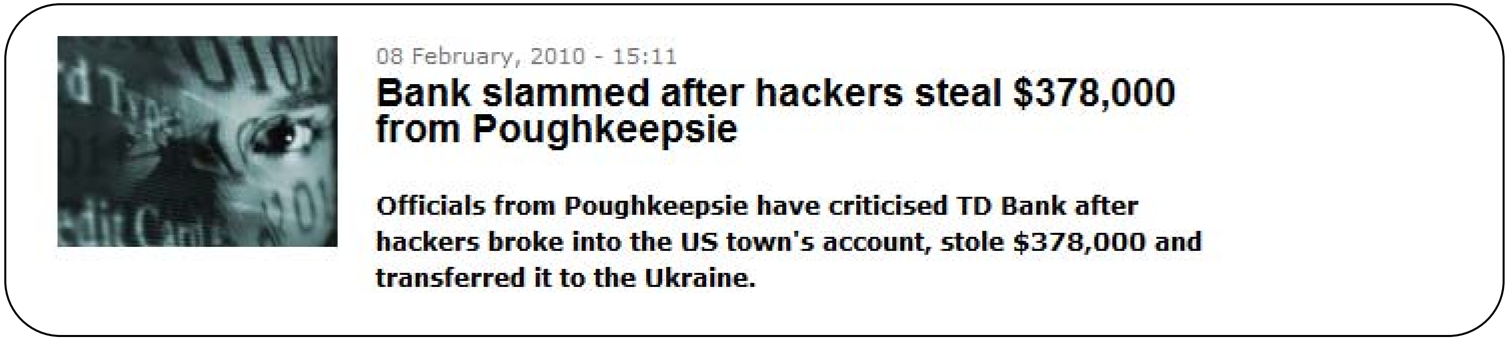
Radix Consulting Corporation

Making Headlines



The Washington Post

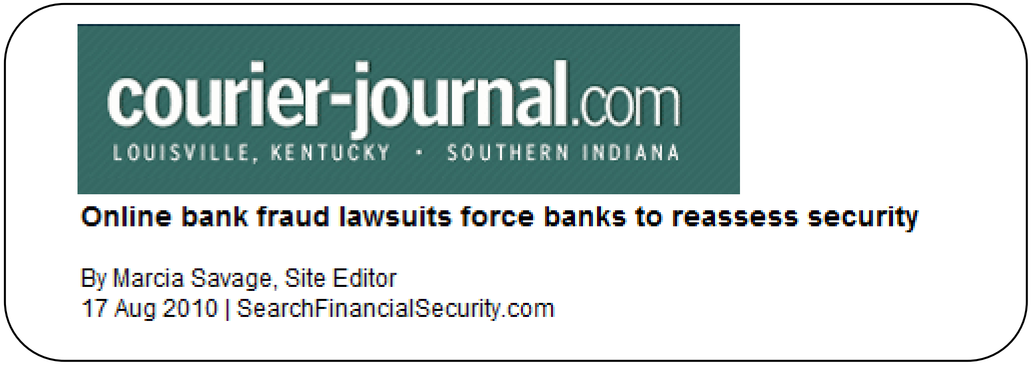
PC Invader Costs Ky. County $415,000



08 February, 2010 - 15:11

Bank slammed after hackers steal $378,000 from Poughkeepsie

Officials from Poughkeepsie have criticised TD Bank after hackers broke into the US town's account, stole $378,000 and transferred it to the Ukraine.



courier-journal.com
LOUISVILLE, KENTUCKY · SOUTHERN INDIANA

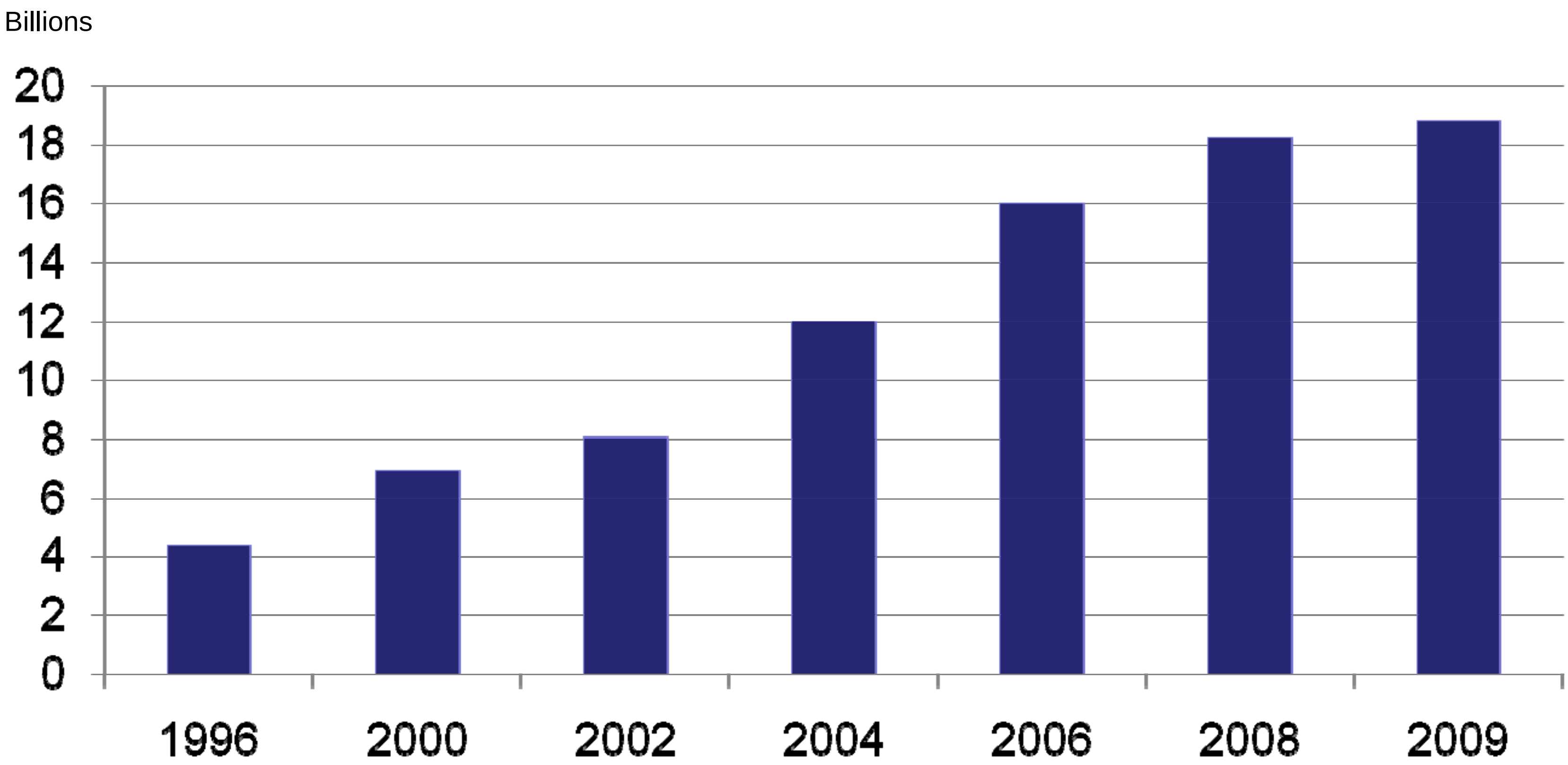
Online bank fraud lawsuits force banks to reassess security

By Marcia Savage, Site Editor
17 Aug 2010 | SearchFinancialSecurity.com

Corporate Account Takeover is the **EQUIVALENT** of ***Identity Theft***

Attempted Losses Due to Online Banking Fraud Reach $100M through 2009

ACH Volume Growth



RADIX CONSULTING CORPORATION
the source for your payments needs

Prevalence of Payments Fraud in 2009

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Checks	**90%**	**93%**	**89%**
ACH debits	25	23	25
Consumer debit/credit cards	20	18	22
Corporate/commercial purchasing cards	17	18	13
ACH credits	7	5	4
Wire transfers	3	3	3

2010 AFP Payments Fraud and Control Survey

ACH Fraud

The Association for Financial Professionals' (AFP) 2010 Payments Fraud and Control survey found that 11% of organizations suffered a financial loss as a result of ACH fraud in 2009 and that they ***"generally did so because they did not follow best practices and/or neglected to execute their own business rules as expeditiously as they should have."***

A look at what is happening

Case Study #1:
Parkinson Construction

- A firm with an estimated $20 million in annual revenue
- Hackers sent $92,000 to nine different money mules
- Financial loss of $18,000 – only two mules succeeded in their task

How did this happen?

- President of Parkinson clicked a link in an e-mail *purporting to be* from the Social Security Administration
- Ended up downloading a copy of the Zeus Trojan
- Thieves had stolen the credentials the president used to administer his construction firm’s bank account online.
- Bank was able to block some of the transactions after being alerted by an anonymous tipster

Case Study #2:
Poughkeepsie Township

- Four transfers worth $378,000 were sent to accounts in the Ukraine on Jan 11th and 12th ($95,000 was recovered)
- On Jan 13th, the bank and the police were called in to investigate
- The town immediately changed all account numbers and the computers involved were removed and given to the Secret Service
- Bank was publically criticized for how they handled situation – no controls to monitor activity and poor communication with the customer

Case Study #3:
Bullet County, Kentucky

- $415,000 were taken from Bullet County’s payroll account
- On June 22nd, someone started making unauthorized funds transfers of $10,000 or less to 25 individuals (money mules) throughout the country
- On June 29th, the bank realized that something was wrong and contacted the receiving banks to reverse the transactions
- This scam used a custom variant of the Zeus Trojan (aka Zbot) that included two new features:
  - Stolen credentials are sent immediately via instant messaging to attackers
  - Malware allowed the criminals to log into the victim’s bank account using the victim’s own internet connection

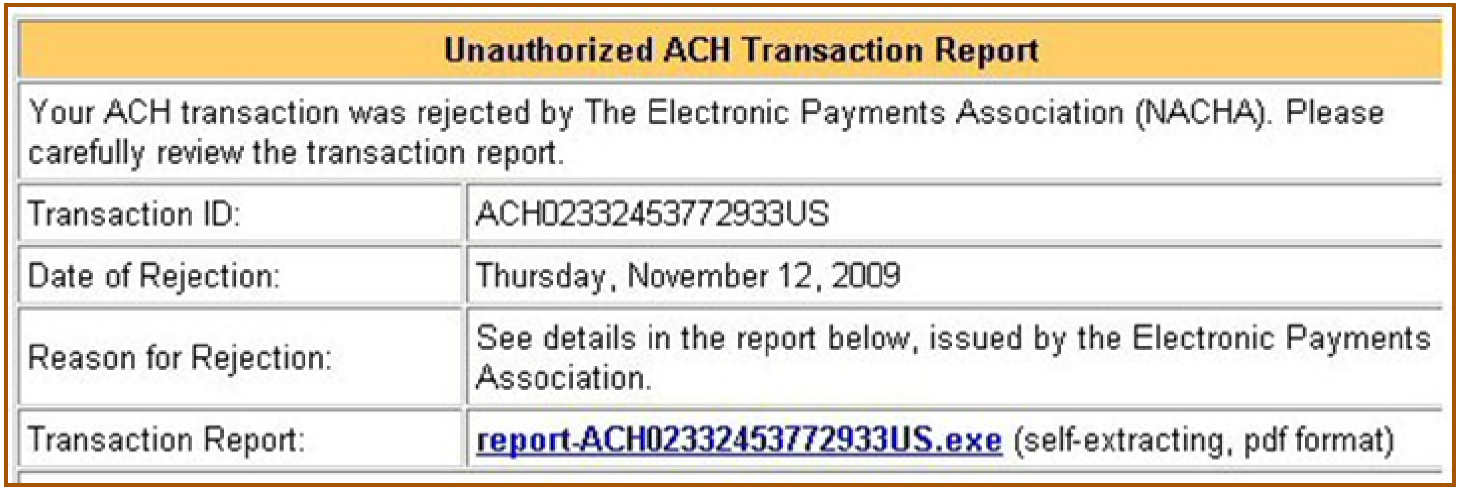
How this scam worked…

- The attackers got the Zeus Trojan on the county treasurer’s PC and used it to steal the username and password the treasurer needed to access email and the county’s bank account
- Attackers logged into the county’s bank account using the treasurer’s internet connection
- Once logged in, they changed passwords as well as email addresses tied to authorized approvers so that any future notifications would be redirected to the attackers

How this scam worked…

- They then created fictitious employees of the county (25 money mules) and created a batch of transactions for approval
- When they logged in to approve the transactions, the bank did not recognize the IP address and sent an email with the challenge passphrase word to an email address now controlled by the attackers
- They used the passphrase to log-in and approve the transactions

The Zeus Trojan



Unauthorized ACH Transaction Report

Your ACH transaction was rejected by The Electronic Payments Association (NACHA). Please carefully review the transaction report.

Transaction ID:	ACH02332453772933US
Date of Rejection:	Thursday, November 12, 2009
Reason for Rejection:	See details in the report below, issued by the Electronic Payments Association.
Transaction Report:	report-ACH02332453772933US.exe (self-extracting, pdf format)

The page, headed "Unauthorized ACH Transaction Report" implores you to download a file that allegedly details the nature of this "transaction" but — if you're a regular reader of the blog, you can guess what happens next. The **Trojan-Backdoor-Zbot** phishing Trojan, once installed, is a keen thief of login credentials.

RADIX
CONSULTING
CORPORATION
the source for your payments needs

What is a money mule?

A person who transfers stolen money or merchandise from one country to another, either in person, through a courier service, or electronically. The term is commonly used to describe on-line scams that prey on victims who are unaware that the money or merchandise they are transferring is stolen. In these scams, the stolen money or merchandise is transferred from the victim's country to the scam operator's country.

Typical targets of Corporate Account Takeover

- Small and Mid sized businesses
- Municipal Governments
- School Districts

Financial Institutions and Companies need to work together

Financial Institutions should…

- Require multifactor authentication log-on features such as secure tokens, access cards, screen entry of sensitive identification data, identity cues
- Provide positive pay/reverse positive pay, ACH debit blocks and debit filters restrictions
- Set limits for file dollar amount and number of files per company and have alerts sent if limits are exceeded
- Implement post-origination software that builds transaction pattern database
- Implement pre-origination software that detects changes in patterns and transactions to new account

RADIX CONSULTING CORPORATION
the source for your payments needs

Financial Institutions should…

- Monitor activity and proactively contact company with mobile and email alerts
- Advise clients of security features offered by FI through client visit and written communications acknowledged by the company
- Offer a Universal Payment Identification Code (UPIC) so your customers can proactively protect account information and still receive ACH payments

What Companies should do to secure sensitive log on credentials…

- Require multifactor authentication log-on features from your financial institution
- Create complex passwords with at least eight characters
- Install and regularly update firewalls, spyware and commercial antivirus software
- Limit administrative rights on users' workstations
- Disable users IDs and passwords for employees on leave or extended vacation
- Conduct new-hire and ongoing information security training

What Companies should do to bolster financial transaction process safeguards…

- Understand and implement security techniques offered by your financial institution
- Implement dual control for all electronic transfers
- Request positive pay/reverse positive pay
- Conduct daily account reconciliation
- Ensure that your system provides an audit trail
- Escalate any suspicious transaction to your financial institution

Questions

Thank you!

Rossana Salaris
rfsalaris@radixconsulting.com
917-453-0693