

Digital Evidence & Financial Crimes

Presented by:

Giovanni Masucci, BCE, MPSC, CLWE, CCPE, CCITP, 132-CI
President/CEO/Sr. Digital Forensic Examiner
National Digital Forensics Inc.

To

NC Office of State Controller GASB Update Seminar
May 19, 2011

Proprietary & Confidential: Unauthorized use without the written consent of National Digital Forensics, Inc. is prohibited. 2011 copyright pending

National Digital Forensics, Inc.

- Providing Digital Forensic Analysis Services to Government, Law Enforcement, Corporations, Law Firms and Academia
- Forensic Consulting: Cases involving Digital Evidence
- Providing Digital Forensic Training & Education
- Expert Witness Services

National Digital Forensics, Inc.

Instructor Introduction

- Giovanni Masucci, CEO/President of NATLDF
- Sr. Digital Forensic Examiner
- State of North Carolina Licensed Counterintelligence since 2003
- Digital Forensic CLE Instructor since 2003
- Attended Federal Law Enforcement Training Center (FLETC)
- Attended WISE & SLATT Trained
- Member US Secret Service Electronic Crimes Task Force (ECTF)
- 2011 President Carolinas HTCIA (High Technology Crime Investigative Association)

National Digital Forensics, Inc.

Program Overview

- Understanding of Financial Crimes
- What is Digital Forensics and the importance to Financial Crimes
- Digital Forensic Process & Financial Crime Evidence
- Impact of Financial Crimes and Social Networking
- Preventing Financial Crimes

National Digital Forensics, Inc.

Our Favorite Crime Scene Investigators!



CSI NY



NCIS



NCIS



CSI MIAMI



CSI LAS VEGAS



CSI MIAMI
Emily Proctor
Raleigh, NC Native



CSI LAS VEGAS

CSI Los Angeles

© CBS Broadcasting Inc. All Rights Reserved
Courtesy of CBS

Understanding White Collar Financial Crimes

National Digital Forensics, Inc.

Defining “White Collar” Financial Crimes

- A person (s) whom are in a position to increase his/her net worth by defrauding others into various activities that benefit only the person or persons initiating the criminal activity.
- Higher Society Status
- Opportunists
- Well educated, intelligent, affluent, confident individuals
- Believe that they are not criminals

National Digital Forensics, Inc.

Financial Crimes Threat

- External Threat
 - Consumer
 - Former Employee
 - Foreign Entity
 - Competitor
 - Criminal Organizations or Individuals
 - Friend/Financial Colleague/Advisor
- Insider Threat
 - Employee
 - Elected Official
 - Appointed Personnel
 - Contractor
 - Vendor

National Digital Forensics, Inc.

What is Actually At Risk

- DATA! DATA! DATA!
- \$\$\$\$\$\$\$\$\$\$\$\$\$\$ and potentially an abundance of it!
- Consumer and Government Financial Loss!

National Digital Forensics, Inc.

Financial Crime Overview

- Identity Theft
- Fraud
- Embezzlement
- Tax Evasion
- Corruption

National Digital Forensics, Inc.

Identity Theft

- Stealing mail
- Opening another person's mail
- Applying for a credit card in someone else's name
- Stealing a credit card or credit card #'s
- Using someone else's credit card
- Stealing social security cards
- Hacking into computers
- Stealing identities online

National Digital Forensics, Inc.

Can You Identify This Device?



National Digital Forensics, Inc



Identity Theft

- **Raleigh man accused of identity theft**
- **Pair charged with using skimmers on Fayetteville ATMs**
- **Ex-DMV worker remains focus of ID theft investigation**
- **Fayetteville pizzeria owner pleads guilty to identity theft**
- **Skimming Devices on Gasoline Pumps increase**

Tax Evasion

- *Individuals moving money off shore
- Individuals who fix the books in order to avoid paying taxes
- Ponzi schemes or pyramid schemes
- Tax protesters who refuse to file taxes
- Financial advisors who recommend fraud to their clients

*Note: Bankruptcy-Off-shore Accounts

National Digital Forensics, Inc.

Tax Evasion/Corruption

- Ex-Easley aide pleads guilty to tax evasion
- Four Charged With Filing False Tax Returns
- Corrupt Official Convicted on Numerous Charges Including:
Tax Evasion
http://www.fincen.gov/law_enforcement/ss/html/Issue%2019-story6.html
- Local Official Sentenced for Tax Evasion
http://www.fincen.gov/law_enforcement/ss/html/Issue%2019-story8.html

National Digital Forensics, Inc.

FRAUD TYPES

- Credit card fraud
- Banking fraud
- Medicaid fraud
- Mortgage fraud
- Insurance fraud
- Computer fraud
- Check fraud
- Mail fraud

National Digital Forensics, Inc.

Public Corruption

- Illegal campaign contributions or finance violations
- Bribery of a government or public official
- Misuse of public office for private gain
- RICO (Racketeering Influenced Corrupt Organization) /racketeering violations
- Schemes to defraud taxpayers
- Illegal kickbacks
- Official misconduct

National Digital Forensics, Inc.

FRAUD CASES

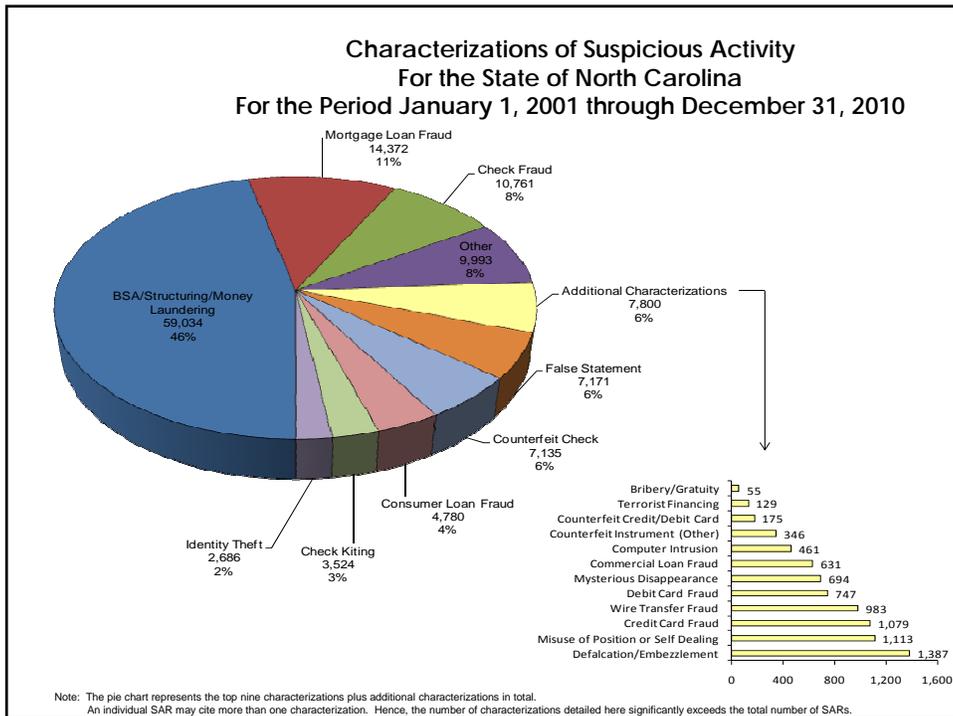
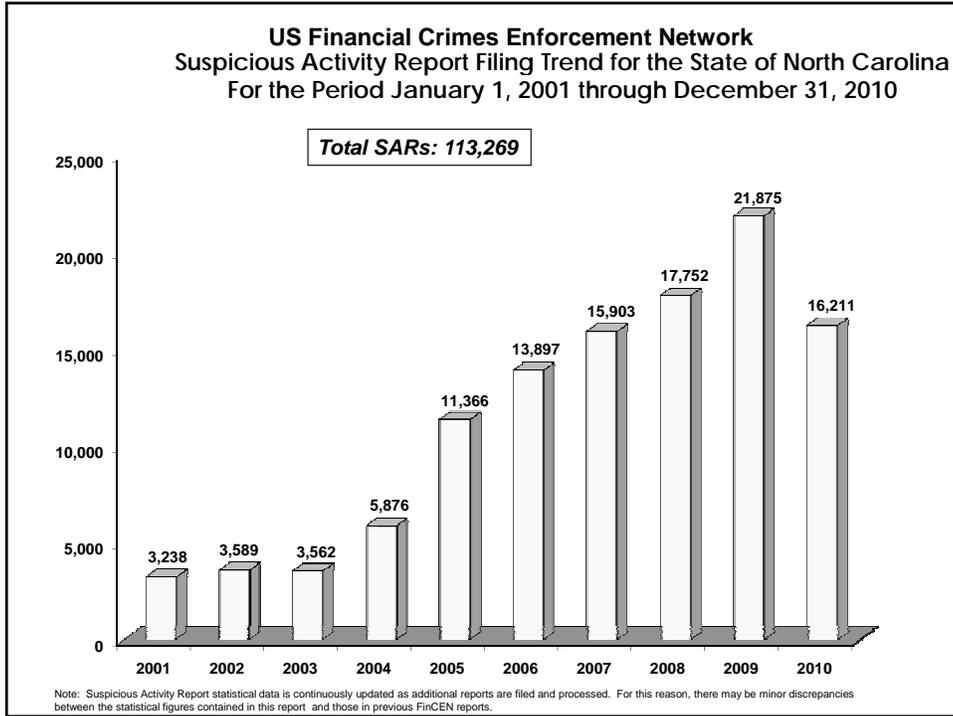
- State roots out \$53M in Medicaid fraud
- Ex-New Hanover ABC chief charged with fraud
- Ex-Cumberland deputy pleads guilty to fraud
- Judge orders ex-Durham official to repay city for fraud
- NC inmates cash in on fraudulent tax returns

National Digital Forensics, Inc.

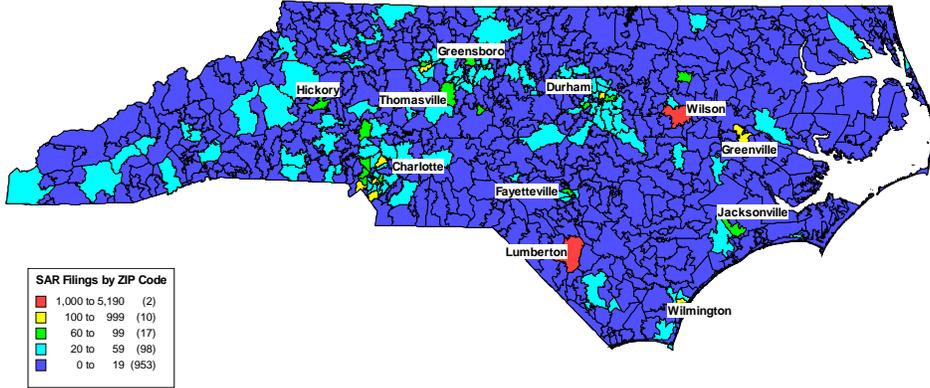
Financial Crime Cases

- **Ex-Harnett teacher sentenced in stock-trading scheme**
- **Johnston man goes from prison to jail on fraud charges**
- **Online dating leads to extortion case, fraud plea**
- **Raleigh man charged with insurance fraud**
- **Wake Forest man charged in bra investment scam**

National Digital

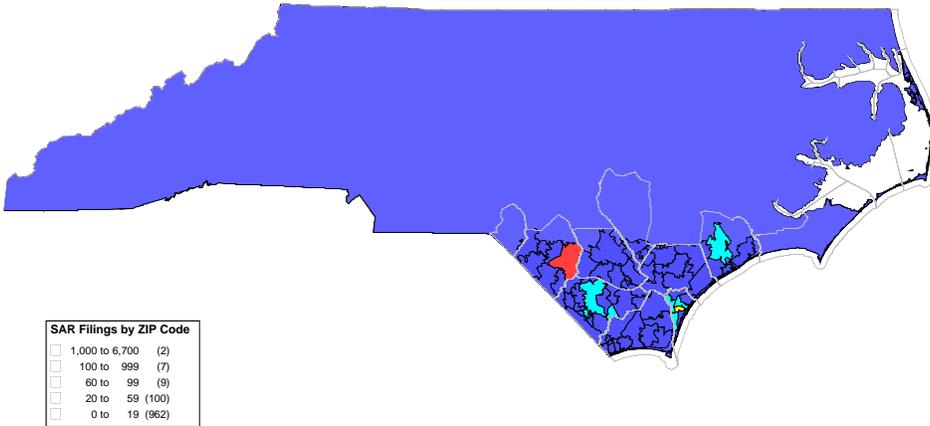


Suspicious Activity Report Geographic Pattern
For the State of North Carolina
For the Period January 1, 2009 through December 31, 2009

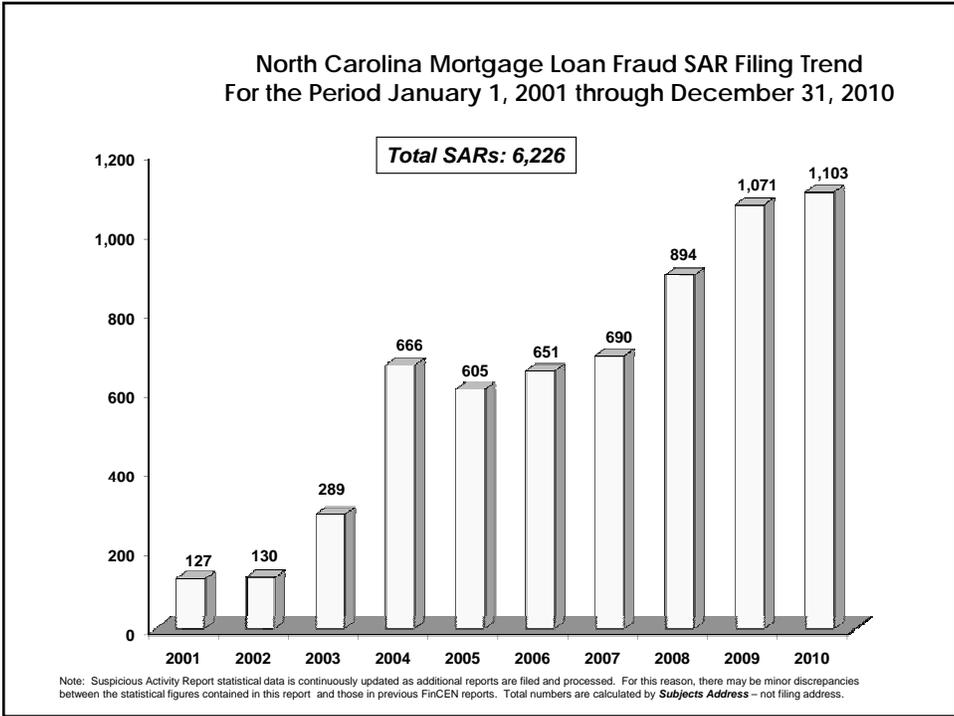


Note: Statistics based on Filer Branch Address

Suspicious Activity Report Geographic Pattern
For the State of North Carolina
For the Period January 1, 2010 through December 31, 2010



Note: Statistics based on Filer Branch Address



Role of Digital Forensics & Financial Crimes

National Digital Forensics, Inc.

What is Digital Forensics?

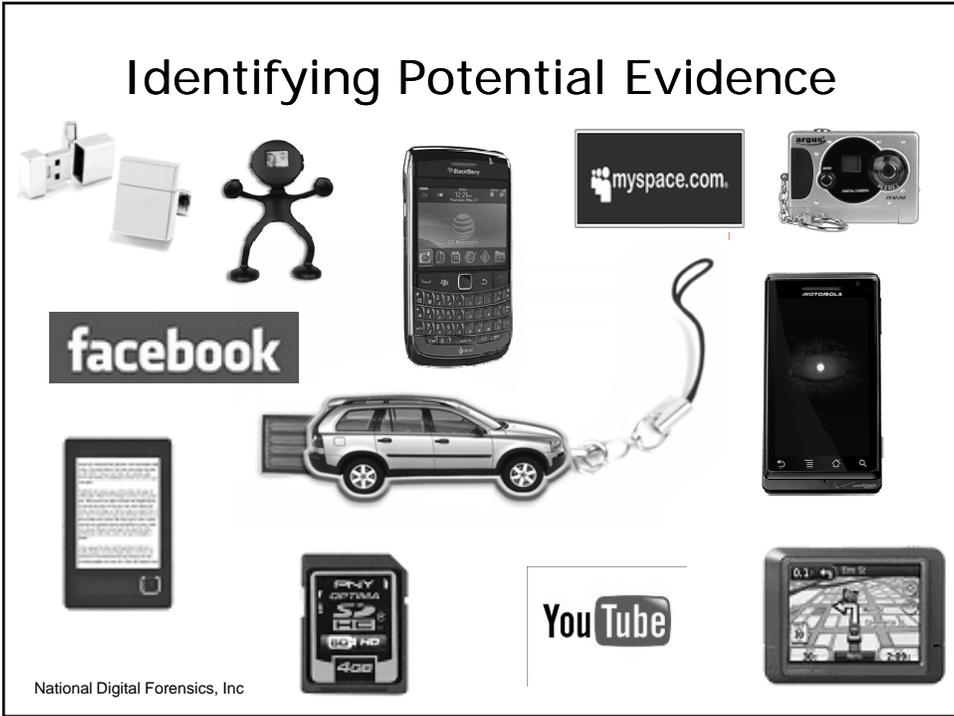
- The recovery of data from any electronic, digital or optical media that's retrievable through process oriented analysis techniques with the intent of recovering potential legal evidence.

National Digital Forensics, Inc.

Types of Devices: Containing Digital Evidence

- Computers, Cell Phones, (I-Phone, BlackBerry, Droid) IPAD
- Firewalls, Wireless Devices, Network Servers
- XBOX, Wii Video Gaming Systems, Toys!
- MP3 Players-IPODS, Security Systems
- Digital Recorders, Digital Cameras, Digital Photo Frames
- Back-up Tapes, Data Storage, E-mail Servers
- Fax Machines, Printers, CD/DVD's, USB External Drives-
 - Flash Sticks, Thumb Drives, Micro Vaults

National Digital Forensics, Inc



Where Can Digital Evidence be obtained?

- Deleted files/Deleted E-mails
- Scanned Documents (data contained in copier/printer hard drive)
- IP Addresses, Passwords, Encrypted files, Hidden Files
- E-Mail Addresses
- Instant Messages/Chat (Skype), G-Mail®, MSN®, Blackberry™ Messenger, Facebook™ Live Chat
- Graphics/Videos (.jpg, .gif, .png,/.avi, .mpeg, .dvr)
- Malware-Keyloggers: Spyware, Eraser Programs
- User History/Internet History/ Deleted History
 - Can provide an Investigator added leads
 - Additional Evidence
 - Potential Criminal Activity

National Digital Forensics, Inc

Digital Forensic Evidence

- Financial Documents
- Transactions
- Credit Card Numbers
- Drivers License Numbers
- Social Security Numbers
- Fraud Documents
- Fraud Tools-Software

National Digital Forensics, Inc

Understanding the Digital Forensic Process

National Digital Forensics, Inc

Case Management

- Initial Contact

- Client; Law Firm, Corporation, LE Agency, Government Agency, Courts

- Define Case

- Type of case?
- Criminal or Civil?
- Court Ordered? Subpoena Involved? Preservation Order? Warrant?
- Parties Involved?
- Potential Conflicts of Interest?
- Agency/Company in Litigation?
- Internal Investigation?
- General Counsel and/or Outside Counsel
- Main point of contact

National Digital Forensics, Inc

Case Management

“Define Services to be performed”

- Perimeters of Examination

- Consultation
- E-Discovery
- On-Site/Off-Site
- Forensic Analysis; Financial
- E-mail Search (relating to one party or several)
- Recover all Financial Software and Databases
- Recover All Deleted Files (Excel, Documents, etc.)
- Affidavit/Depositions/Testifying
- Timeline to complete tasks

National Digital Forensics, Inc

Be Aware of “Applicable Regulations”

- Are there applicable State & Federal Laws that apply to your Agency??
 - Regulatory & Privacy Regulations
 - HIPPA (Dealing w/Patient Records Confidentiality)
 - ERISA (Employee Retirement Income Security Act)
 - Sarbanes Oxley (SOX) Financial Accountability
 - PCI (Payment Card Industry)

National Digital Forensics, Inc

Case Management “Case Impact”

- Understanding Your Case
- Criminal or Civil:
- Identifying Known Digital Evidence
- What Format is the Digital Evidence In?
- Do you have original media or access to where Digital Evidence was obtained from?
- On-Line Evidence Gathering

National Digital Forensics, Inc

Case Management

Digital Forensic Examination Process

- Identifying/Preserving
- Collecting
- Examination
- Analyzing
- Reporting

National Digital Forensics, Inc

Case Management Identifying/Preserving

Processing Potential Evidence

- Documenting (Physical Inspection)
 - Chain of Custody Procedures
 - Consent Form
 - Assigned Case Identifier/Evidence Number
 - Digital Camera
 - Journal or Word Document (Case Log)
- Securing
 - Logs
 - Packaging
 - Identifying Tags/Label

National Digital Forensics, Inc

Case Management Collecting

- Imaging data and creating Forensic Formats for Examination
- *Ensuring All Data to be collected is Write Protected
- Volatile Data
 - Documentation on how it was collected
 - * There will be times when data must be directly accessed which is acceptable as long as its' documented.

National Digital Forensics, Inc

Case Management Collecting

- Acquiring Forensic Image (s)
 - Hard Drives-Internal/External
 - Servers
 - Cell Phones
 - Smart Phones
 - CD/DVD's
 - USB Devices

National Digital Forensics, Inc

Case Management Examination

- Start Processing Evidence Items;
 - Identifying areas of interest
 - Keyword Search
 - E-mails
 - Internet History
 - Deleted History, Files
 - Graphics
- Preview Evidence

National Digital Forensics, Inc

Case Management "Types of Analysis"

- Malware Analysis
- E-Mail Analysis
- Social Network Analysis
- Internet History Analysis
- Deleted History Analysis
- Registry Analysis
- Graphics Analysis
- Financial Analysis
- Comparison Analysis

National Digital Forensics, Inc

Case Management

Industry Recognized Digital Forensic Tools

- ✓ Encase™ by Guidance Software Inc.
- ✓ FTK™ by Access Data
- ✓ Internet Evidence Finder™
- ✓ Webcase™
- ✓ Logicube™ Forensic Tools
- ✓ Paraben™ Forensic Software Tools
- ✓ WetStone™ Forensic Software

National Digital Forensics, Inc

Case Management-Reporting

- Reporting Process
 - Findings
 - Bookmarked & Exported
 - Create Report; soft copy
 - Burn Report to Evidence Grade CD/DVD
 - Additional Copies for Lab, Court and other parties involved as required
 - Deliver to Client continuing Chain of Custody Procedures

National Digital Forensics Inc

Case Management-Reporting

- Facts on Data Recovered
- Weekly Status Updates (if applicable)
- Summary Report-Soft Copy/Conference call/Client Meeting
- Reports-On Analysis Completed
- Technical Report-For Court if Necessary

National Digital Forensics, Inc

Testifying

- Depositions/Affidavits
- Court Appointed Expert
- Expert Witness
 - Certified Board
 - Courtroom/Jury
- Presentations

National Digital Forensics, Inc.

Financial Crimes & Social Networking Impact

National Digital Forensics, Inc



"On the Internet, nobody knows you're a dog."

The above cartoon by Peter Steiner has been reproduced from page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20) only for academic discussion, evaluation, research and complies with the copyright law of the United States as defined and stipulated under Title 17 U. S. Code.

National Digital Forensics, Inc.

**WHAT IS SOCIAL NETWORKING?
Or Should I state; “What is Social
Engineering?”**

National Digital Forensics, Inc.

Social Networking

**A WAY FOR A DIGITAL FORENSIC
EXAMINER TO GATHER EVIDENCE
(INFORMATION) ABOUT YOU, YOUR
FAMILY, YOUR FRIENDS, YOUR
COWORKERS, YOUR SIGNIFICANT
OTHER, YOUR LIFESTYLE AND
EVERYONE ELSE'S THAT MAY BE
PERTINENT TO A CASE!**

By Giovanni Masucci

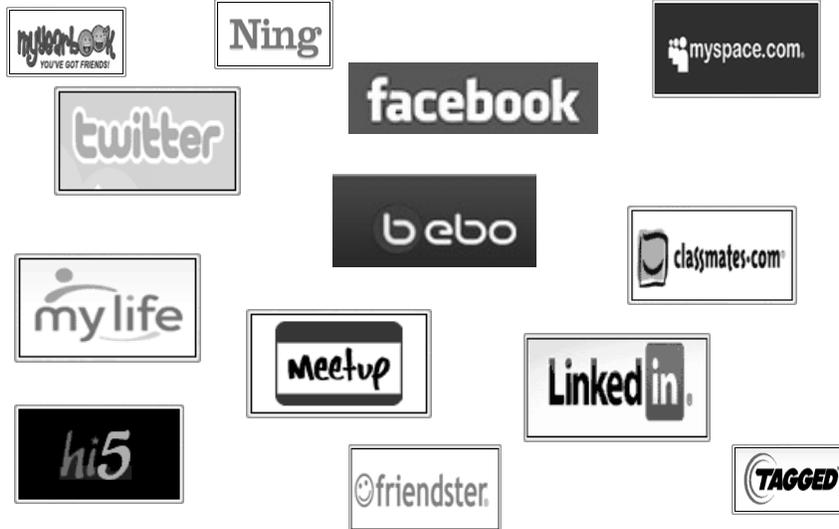
National Digital Forensics, Inc.

Social Engineering

A way for someone to talk his/her way into gaining information thru a level of trust, knowledge that will lead to their benefit and potential criminal activity.

National Digital Forensics, Inc.

Social Networking Sites



National Digital Forensics, Inc.

2010 Internet Crimes Report

<u>Type</u>	<u>Percent</u>
1. Non-delivery Payment/Merchandise	14.4%
2. FBI-Related Scams	13.2%
3. Identity Theft	9.8%
4. Computer Crimes	9.1%
5. Miscellaneous Fraud	8.6%
6. Advance Fee Fraud	7.6%
7. Spam	6.9%
8. Auction Fraud	5.9%
9. Credit Card Fraud	5.3%
10. Overpayment Fraud	5.3%

Statistics provided by NWC3 National White Collar Crime Center & the FBI

National Digital Forensics Inc.

Social Networking "Employer Impact"

Impact to operations

- Business Intelligence
- Cyber Security Risks
 - Phishing Scams
 - Identity Theft
- Physical Security Risks
- Leading to Criminal Activity

National Digital Forensics, Inc

Social Networking "Personal Impact"

Once on the Web, always on the Web!

- Embarrassment
- Harassment
- Identity Theft
- Property Theft
- Scammed
- Separation
- Divorce
- Physical Harm
- Job Loss
- Conviction

National Digital Forensics, Inc

Social Networking "Digital Evidence"

A Digital Forensic Examiner will acquire Social Networking artifacts utilizing specialized Forensic Software obtaining Web-sites/Pages or Partial information in relation to the case.

National Digital Forensics, Inc

Forensic Analysis of Financial Crimes

- Searching for evidence; search for documents such as spreadsheets and images of checks and/or potentially fraudulent financial materials.
- Search Documents for financial applications such as MS Money, Quicken, and QuickBooks may also contain items of interest or any other type of financial software.
- Search for Credit Card Numbers and Social Security Card Numbers

National Digital Forensics, Inc.

Social Networking Evidence “Digital Forensic Tools”

Forensic Analysis Tools

Acquires:

- Facebook™ Live Chat Messages
- Facebook™ Page Fragments
- Facebook™ Email “Snippets”
- MSN Live Messenger®
- Yahoo Chat®
- Yahoo Webmail Chat®
- Google Chat®
- Gmail E-mail®
- Limewire® Files and Search History
- MySpace™ Chat
- Bebo® Chat
- AOL Instant Messenger®
- Yahoo® & Hotmail ®E-Mail

National Digital Forensics, Inc.

Social Networking "Digital Evidence"

- Access to Internet Sites
- Access to Pictures being Posted
- Profiles Created
- E-Mail Accounts
- Friends
- Friend Postings
- Photos/Videos
- Wall Info
- Information Public or Private Setting

National Digital Forensics, Inc

PREVENTING FINANCIAL CRIMES

National Digital Forensics, Inc.

Protect Your Information!

- Having key IT, Physical Security and Evidence Handling Policies in place
- Audit Controls in Place
- Access Controls
 - Biometrics
 - Employees limited access to certain areas
- Change passwords on Computers every 30 days
- Hard Drive Encryption
- Data Encryption
- Secured Physical Access to Servers
- Secured Physical Access to Telephony Room (switch board located; T1 Lines, Cable Lines)
- Firewalls/Antivirus Programs/Network Monitoring of Internal And External Threats
- Monitor your Social Networking Account Controls
 - Limiting Internet usage

National Digital Forensics, Inc.

Preventing Financial Crimes

PCI

- Identify data storage risks on computer systems
- Prevent security breaches that result in the theft of customers' credit and debit card numbers.
- Prepare for the unexpected-Unencrypted credit card data exposed during transaction, data storage-backup

National Digital Forensics, Inc.

Preventing Financial Crimes

- Assessing Agency/Department and Organizational Role
- Don't be reactive be proactive!
- Internal Agency Review
- Monitoring current trends
- Identifying False Claims before they are paid

National Digital Forensics, Inc.

Preventing Financial Crimes

- Verifying & Validation: Identifying duplicate names, addresses, soc sec numbers patterns of inconsistencies and redundancies.
- Addressing critical infrastructure data systems that need updating.
- Remember prevention doesn't start with the Investigator but with every employee.
- Training, Training, Training!

National Digital Forensics, Inc.

Preventing Financial Crimes

- Don't leave your LAPTOP IN YOUR VECHILE!
- Don't leave any information of value in your vehicle at anytime!
- Many crimes happen because opportunity presents itself!

National Digital Forensics, Inc.

References

- <http://www.fbi.gov/stats-services/publications/financial-crimes-report-2009>
- Financial Crimes Enforcement Network
<http://www.fincen.gov/>
- Bank Secrecy Act (BSA)
http://www.fincen.gov/statutes_regs/bsa/
- http://www.fincen.gov/news_room/rp/files/sar_tti_16.pdf.
- NWC3 <http://www.nw3c.org/>

National Digital Forensics, Inc.

Questions?

Questions?

Questions?

National Digital Forensics, Inc

Thank You!

Giovanni Masucci, CEO/President
Sr. Digital Forensic Examiner
National Digital Forensics Inc.
Raleigh, North Carolina
(919)754-8644 (Office)
(877)754-8644 Toll free
(919)961-8007 (Mobile)
E-Mail: gmasucci@natldf.com
Web-Site: www.natldf.com

National Digital Forensics, Inc