

NYS Information Security Breach and Notification Act



March 23, 2006

Mara B. Ginsberg

Counsel

Cyber Security & Critical Infrastructure
Coordination

What Prompted this NY Law?

- Constant tide of identity theft >3 million
- ChoicePoint- more than 9,000 New Yorkers had their personal information exposed
- California had a law but New York did not
- ChoicePoint didn't notify New Yorkers until the story made national news
- DSW Shoe outlet theft of customer credit card information from the 2004-05 holiday season (thousands of New Yorkers)

- Feb. 15, 2005 ChoicePoint- Bogus accounts established by ID thieves 145,000
- Feb. 25 , 2005 Bank of America Lost backup tape 1,200,000
- Feb. 25, 2005 PayMaxx Exposed online 25,000
- March 8, 2005 DSW/Retail Ventures Hacking 100,000
- March 10, 2005 LexisNexis Passwords compromised 32,000
- March 11, 2005 Univ. of CA, Berkeley Stolen laptop 98,400
- March 11, 2005 Boston College Hacking 120,000
- March 12, 2005 NV Dept. of Motor Vehicle Stolen computer 8,900
- March 20, 2005 Northwestern Univ. Hacking 21,000
- March 20, 2005 Univ. of NV., Las Vegas Hacking 5,000
- March 22, 2005 Calif. State Univ., Chico Hacking 59,000
- March 23, 2005 Univ. of CA, San Francisco Hacking 7,000
- March 28, 2005 Univ. of Chicago Hospital Dishonest insider unknown
- April, 2005 Georgia DMV Dishonest insider 465,000
- April 5, 2005 MCI Stolen laptop 16,500
- April 8, 2005 Eastern National Hacker 15,000
- April 8, 2005 San Jose Med. Group Stolen computer 185,000
- April 11, 2005 Tufts University Hacking 106,000

- April 12, 2005 LexisNexis Passwords compromised Additional 280,000
- April 14, 2005 Polo Ralph Lauren/HSBC Hacking 180,000
- April 14, 2005 Calif. Fastrack Dishonest Insider 4,500
- April 15, 2005 CA Dept. of Health Services Stolen laptop 21,600
- April 18, 2005 DSW/ Retail Ventures Hacking Additional 1,300,000
- April 20, 2005 Ameritrade Lost backup tape 200,000
- April 21, 2005 Carnegie Mellon Univ. Hacking 19,000
- April 26, 2005 Mich. State Univ's Wharton Center Hacking 40,000
- April 26, 2005 Christus St. Joseph's Hospital Stolen computer 19,000
- April 28, 2005 Georgia Southern Univ. Hacking "tens of thousands"
- April 28, 2005 Wachovia,
Bank of America,
PNC Financial Services Group and
Commerce Bancorp Dishonest insiders 676,000
- April 29, 2005 Oklahoma State Univ. Missing laptop 37,000
- May 2, 2005 Time Warner Lost backup tapes 600,000
- May 4, 2005 CO. Health Dept. Stolen laptop 1,600 (families)
- May 5, 2005 Purdue Univ. Hacking 11,360
- May 7, 2005 Dept. of Justice Stolen laptop 80,000
May 11, 2005 Stanford Univ. Hacking 9,900
- May 12, 2005 Hinsdale Central High School Hacking 2,400
- May 16, 2005 Westborough Bank Dishonest insider 750
- May 18, 2005 Jackson Comm. College, Michigan Hacking 8,000

December 5, 2005
copyright CSCIC

- May 19, 2005 Valdosta State Univ., GA Hacking 40,000
- May 20, 2005 Purdue Univ. Hacking 11,000
- May 26, 2005 Duke Univ. Hacking 5,500
- May 27, 2005 Cleveland State Univ. Stolen laptop 44,420
- May 28, 2005 Merlin Data Services Bogus acct. set up 9,000
- May 30, 2005 Motorola Computers stolen unknown
- June 6, 2005 CitiFinancial Lost backup tapes 3,900,000
- June 10, 2005 Fed. Deposit Insurance Corp. (FDIC) Not disclosed 6,000
- June 16, 2005

- CardSystemsHacking40,000,000
- June 17, 2005 Kent State Univ. Stolen laptop 1,400
- June 18, 2005 Univ. of Hawaii Dishonest Insider 150,000
- June 22, 2005 Eastman Kodak Stolen laptop 5,800
- June 22, 2005 East Carolina Univ. Hacking250
- June 25, 2005 Univ. of CT (UCONN) Hacking72,000
- June 28, 2005 Lucas Cty. Children Services (OH) Exposed by email 900
- June 29, 2005 Bank of America Stolen laptop 18,000
- June 30, 2005 Ohio State Univ. Med. Ctr. Stolen laptop 15,000
- July 1, 2005 Univ. of CA, San Diego Hacking3,300
- July 6, 2005 City National Bank Lost backup tapes unknown
- July 7, 2005 Mich. State Univ. Hacking27,000
- July 19, 2005 Univ. of Southern Calif. (USC) Hacking270,000 possibly accessed; "dozens" exposed
- July 21, 2005 Univ. of Colorado-Boulder Hacking42,000
- July 30, 2005 San Diego Co. Employees Retirement Assoc. Hacking33,000
- July 30, 2005 Calif. State Univ., Dominguez Hills Hacking9,613
- July 31, 2005 Cal Poly-Pomona Hacking31,077
- Aug. 2, 2005 Univ. of Colorado Hacking36,000
- Aug. 9, 2005 Sonoma State Univ. Hacking 61,709
- Aug. 9, 2005 Univ. of Utah Hacking100,000
- Aug. 10, 2005 Univ. of North Texas Hacking39,000
- Aug. 17, 2005 Calif. State University, Stanislaus Hacking900
- Aug. 19, 2005 Univ. of Colorado Hacking49,000
- Aug. 22, 2005 Air Force Hacking33,300
- Aug. 27, 2005 Univ. of Florida, Health Sciences Center/ChartOne Stolen Laptop 3,851
- Aug. 30, 2005 J.P. Morgan, Dallas Stolen Laptop Unknown
- Aug. 30, 2005 Calif. State University, Chancellor's Office Hacking154
- Sept. 10, 2005 Kent State Univ. Stolen Computers100,000
- Sept. 15, 2005 Miami Univ. Exposed Online 21,762

December 5, 2005
copyright CSCIC

- Sept. 16, 2005 ChoicePoint (2nd notice, see [2/15/05](#) for 145,000) ID thieves accessed; also misuse of IDs & passwords. 9,903
- Sept. 17, 2005 North Fork Bank, NY Stolen laptop (7/24/05) with mortgage data 9,000
- Sept. 19, 2005 Children's Health Council, San Jose CA Stolen backup tape 5,000 - 6,000
- Sept. 22, 2005 City University of New York Exposed online 350
- Sept. 23, 2005 Bank of America Stolen laptop with info of Visa Buxx users (debit cards) Not disclosed
- Sept. 28, 2005 RBC Dain Rauscher Illegitimate access to customer data by former employee 100+ customers' records compromised out of 300,000
- Sept. 29, 2005 Univ. of Georgia Hacking At least 1,600
- Oct. 15, 2005 Montclair State Univ. Exposed online 9,100
- Oct. 21, 2005 Wilcox Memorial Hospital, Hawaii Lost backup tape 130,000
- Nov. 1, 2005 Univ. of Tenn. Medical Center Stolen laptop 3,800
- Nov. 4, 2005 Keck School of Medicine, USC Stolen computer 50,000
- Nov. 5, 2005 Safeway, Hawaii Stolen laptop 1,400 in Hawaii, perhaps more elsewhere
- Nov. 8, 2005 ChoicePoint Bogus accounts established by ID thieves Total affected now reaches 162,000 (See [Feb. 15](#) & [Sept. 16](#))
- Nov. 9, 2005 TransUnion Stolen computer 3,623
- Nov. 11, 2005 Georgia Tech Ofc. of Enrollment Services Stolen computer, Theft 10/16/05 13,000
- Nov. 19, 2005 Boeing Stolen laptop with HR data incl. SSNs and bank account info. 161,000

Known Private information exposure since Feb 2005

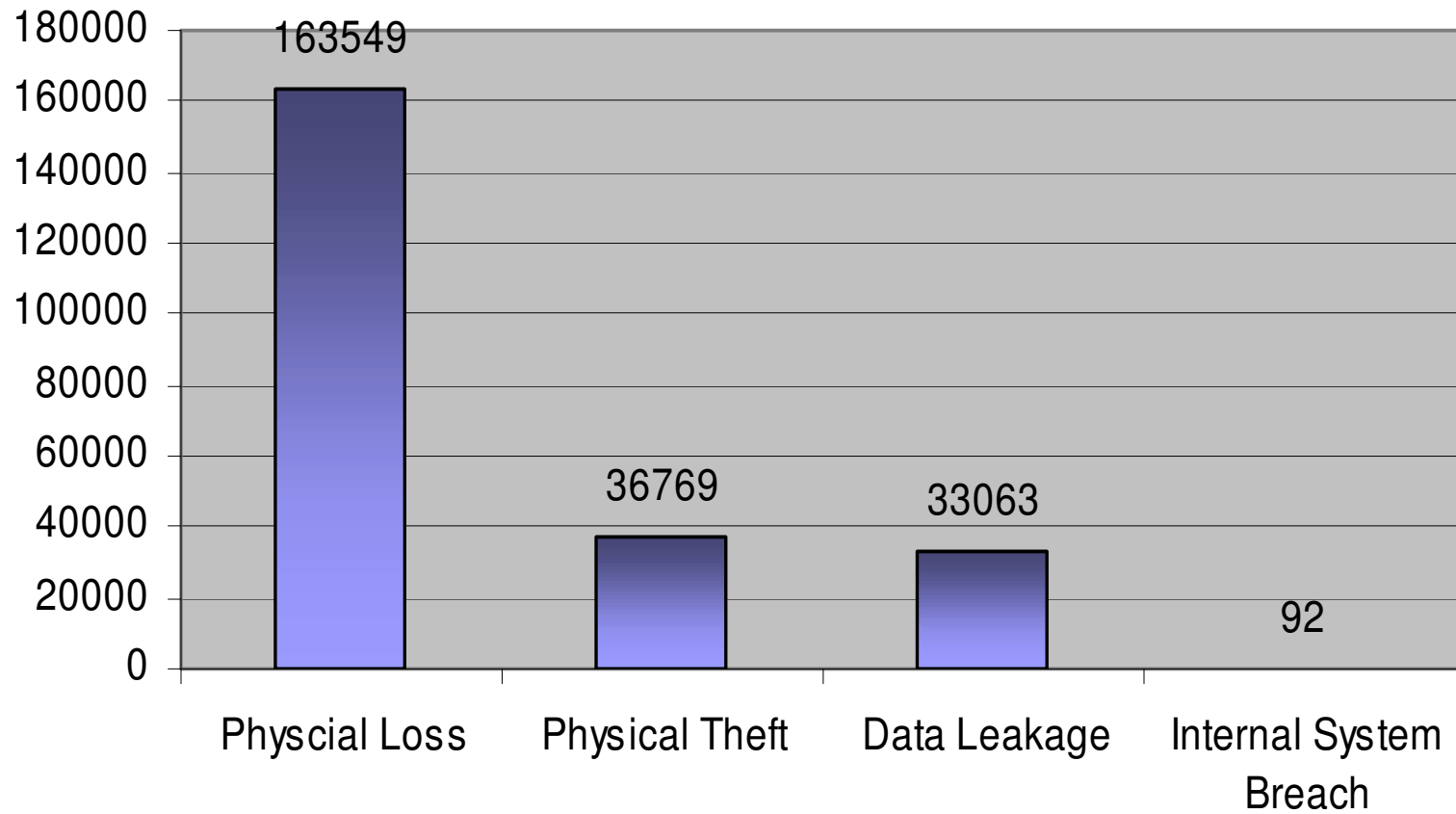
51,668,622



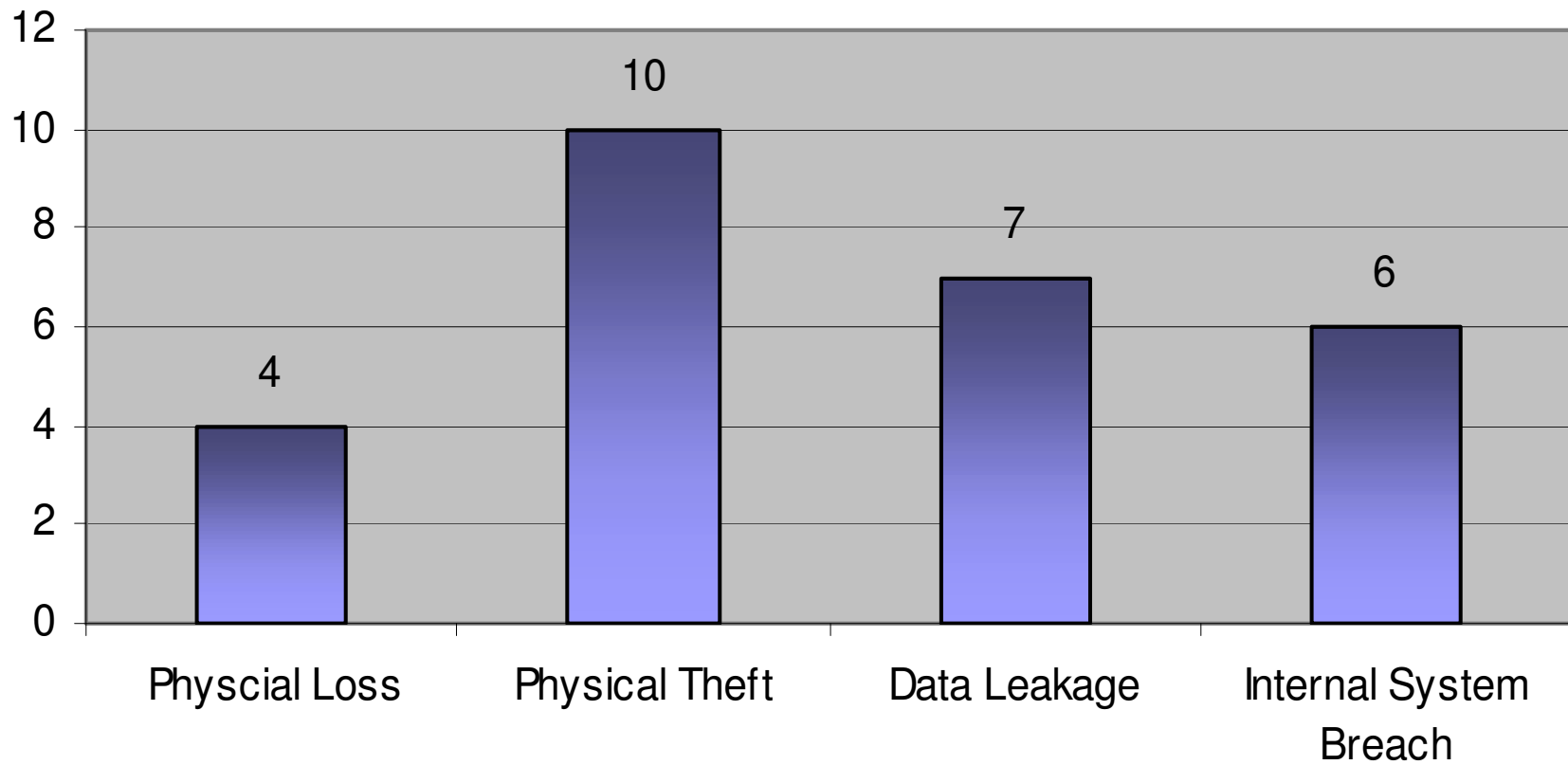
December 5, 2005
copyright CSCIC

Category_Name	Total Number of Affected NYS Residents	Count of Entity Reports
Physical Loss	163,549	4
Physical Theft	36,769	10
Data Leakage	33,063	7
Internal System Breach	92	6

Total Number of Affected NYS Residents



Count of Entity Reports

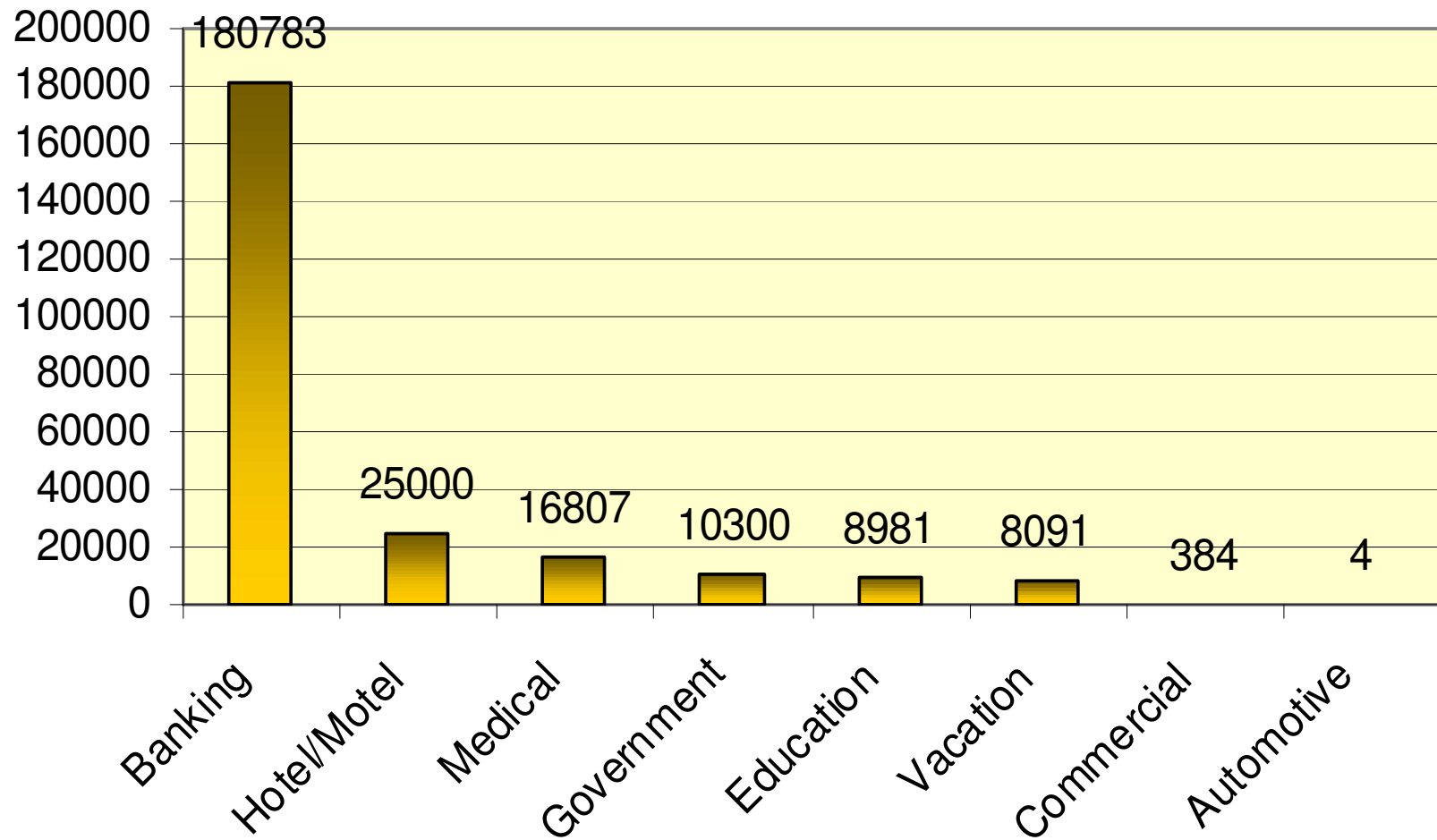


Vertical_Name	Total Number of Affected NYS Residents	Count of Entity Reports
Banking	180,783	13
Hotel/Motel	25,000	1
Medical	16,807	2
Government	10,300	2
Education	8,981	4
Vacation	8,091	1
Commercial	384	7
Automotive	4	1

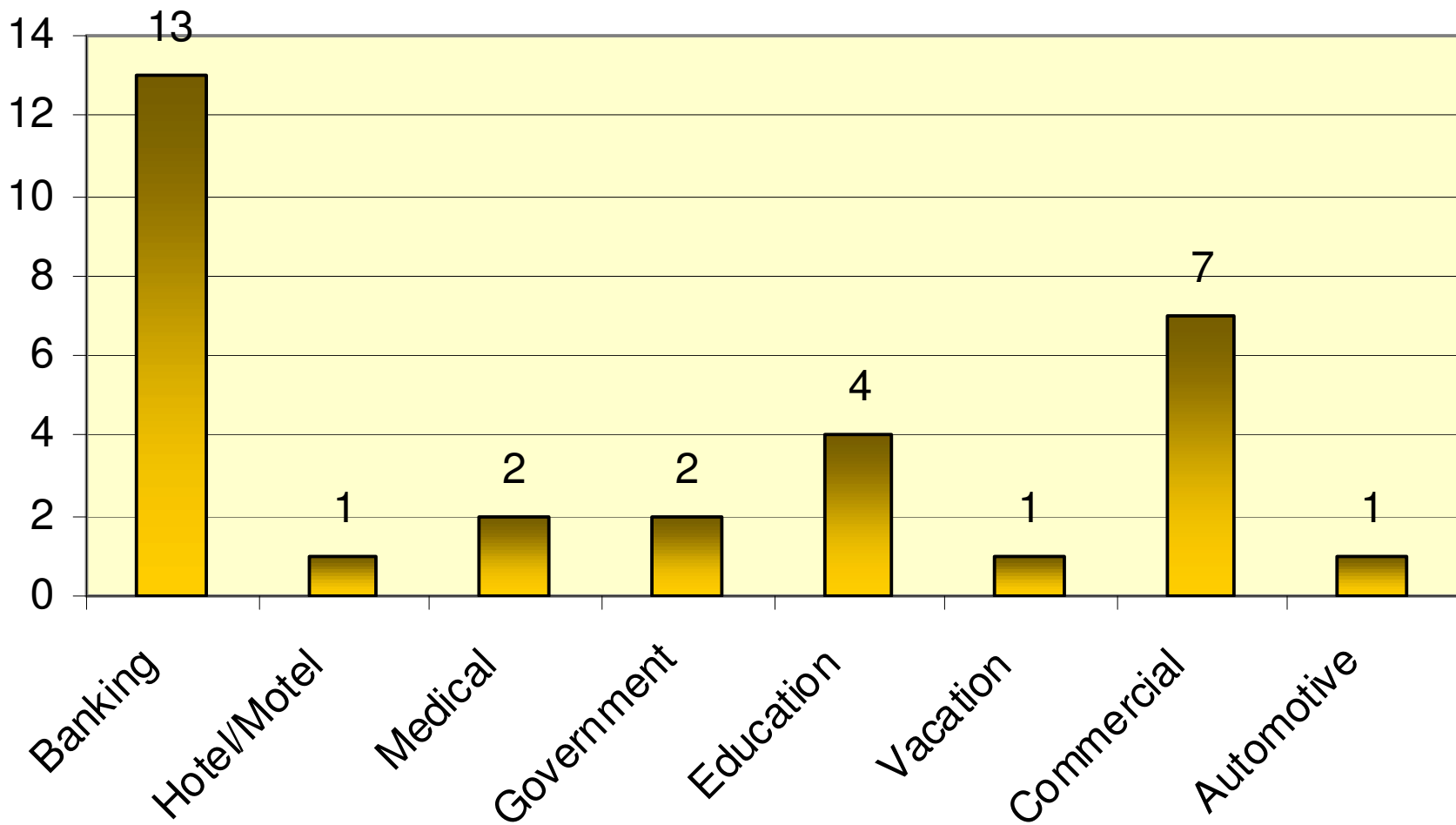
December 5, 2005
copyright CSCIC

- **E&Y appears to be having a bad month.....**
- **Ernst & Young loses four more laptops**
- Gear pinched while auditors dined
- By Ashlee Vance in Mountain View
- Published Sunday 26th February 2006 20:36 GMT
- **Ernst and Young appears set on establishing a laptop loss record in February. The accounting giant has lost four more systems, according to a report in the Miami Herald.**
- **A group of Ernst and Young auditors toddled off for lunch on 9 February, leaving their laptops in an office building conference room. According to security footage, two men entered the conference room a couple of minutes after the Ernst and Young staffers left and walked off with four Dell laptops valued at close to \$8,000, the paper reported.**
- **This theft follows a higher-profile incident in which an Ernst and Young employee lost his laptop containing the social security numbers and other personal information of customers. One such customer happened to be Sun Microsystems CEO Scott McNealy who was told that his social security number had been compromised - an incident first reported here.**
- **The laptop with McNealy's data was stolen from an employee's car, according to Ernst and Young.**
- **It's unclear what type of security Ernst and Young had on the four laptops pinched in Miami. It maintains that the laptop containing McNealy's information was password protected.**
- **Ernst and Young has failed to issue a public statement about these breaches despite being a major advocate of transparency in such issues in its role as an auditor and corporate advisor. ®**

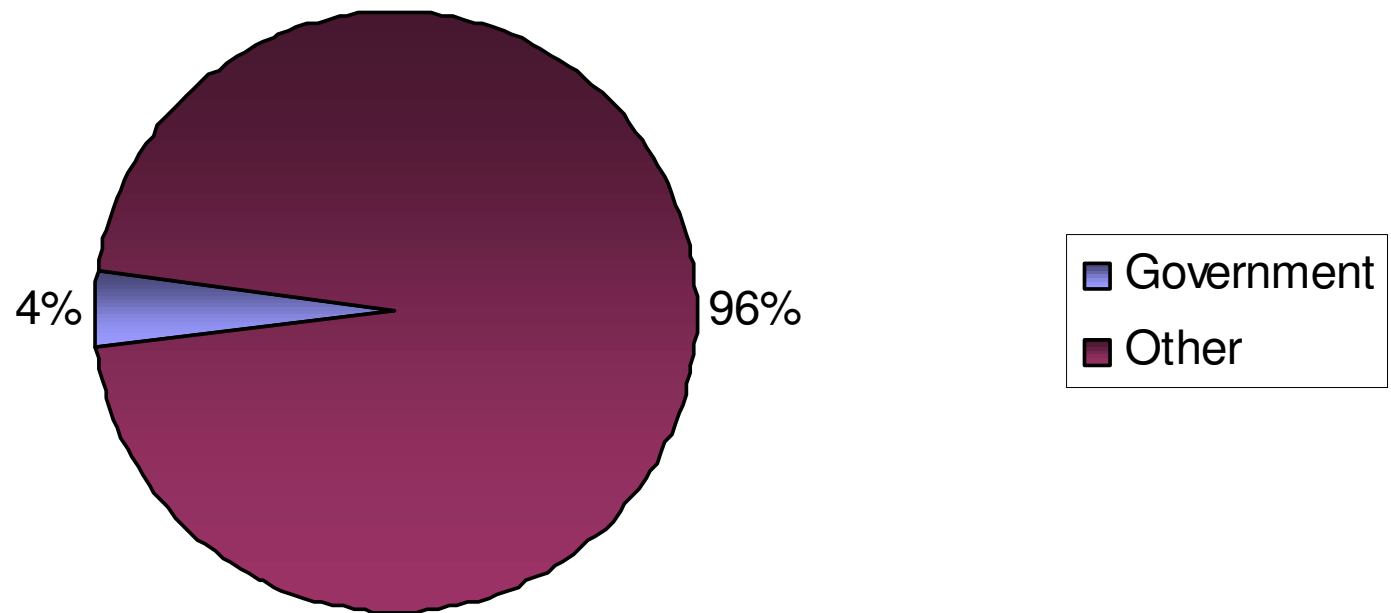
Total Number of Affected NYS Residents



Count of Entity Reports



Total Number of Incidents Affecting NYS Residents



Total Number of Affected NYS Resident Incidents	Government	Other
250,350	10,300	240,050

Information Security Breach and Notification Act

- Chapters 442 and 491 of the Laws of 2005
- Adds new section 208 to the State Technology Law
- Adds new article 39-F to the General Business Law

Information Security Breach and Notification Act

- Chapters 442 & 491 of the Laws of 2005
- Adds new section 208 to the State Technology Law
- Adds new article 39-F to the General Business Law

Definitions

- ***Private Information***- is unencrypted personal information + 1 or more:
 - Social security #
 - Driver's license number or non-driver ID
 - Account number, credit or debit card # + security code, access code or password which permits access to an individual's financial account

State entity

- State board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state except:
 - The judiciary
 - Cities, counties, municipalities, villages, towns and other local agencies
 - (however, cities etc must adopt a notification policy or local law consistent with this law no later than 120 days from the effective date of C442.– they have 240 days from 8-9-05)

Person or Business

- Any Person or Business which conducts business in NY and which owns or licenses computerized data which includes private information shall disclose any breach or private information to NY residents.
- Any person or business which maintains computerized data with private information



December 5, 2005
copyright CSCIC

Has information been acquired?

- Some factors to consider:
 - Indications that the information is in the physical possession and control of someone unauthorized i.e. lost or stolen computer
 - Indications that the information has been downloaded or copied
 - Indications that the information was used by an unauthorized individual i.e. fraudulent accounts opened or instances of identity theft

What does the law require of businesses?

- Disclose the breach to a New York resident whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization

How to notify

- Notice shall be provided to the affected person by one of the following methods:
 - Written notice
 - Electronic notice (provided there was a previous express consent to this method) and a log of electronic notice must be maintained
 - Telephone notice- provided the SE keeps a log

When to Notify

- Do consider:
 - Most Expedient Time Possible
 - Without Unreasonable Delay
 - But after necessary measures to determine the scope of the breach and restore integrity
 - Delay if law enforcement determines it impedes a criminal investigation

Substitute Notice

– Substitute notice if

- the State Entity or Business demonstrates to the AG that the cost of providing notice >\$250,000 or > 500,000 individuals need notification or the business doesn't have sufficient contact information) All of the following:
 - Email
 - Conspicuous posting on the Business website
 - Notification to major statewide media

Notification

Notification must include (see form on our website www.cscic.state.ny.us) :

- Contact information for the Business making the notice
- Description of the categories of information that were or are reasonably believed to have been acquired including:
 - Specification of elements of acquired information

Notification Procedures

- The Business must notify the AG, the CPB and CSCIC (without delaying the notification to the individuals) of:
 - The timing of the notification
 - The content of the notification
 - The distribution of the notification
 - The approximate number of individuals who will be notified

Consumer Reporting Agencies

- If > 5,000 New York residents are to be notified at one time, then State Entity or Business must notify the consumer reporting agencies of:
 - Timing
 - Content
 - Distribution
 - Approximate number of people impacted

Business Notification Requirements

AG may bring an action on behalf of people of NY to enjoin a violation

- AG may receive damages for actual costs or losses
- For willful violation there may be a civil penalty for failure to notify of the greater of \$5,000 or \$10/per instance up to \$150,000

Is there ever a question of what entity provides the notice?

- Digital break-in at CardSystems was publicly disclosed by MasterCard on June 17.
- Intruders got access to details on about 40 million credit cards.
- Records of more than 200,000 cards are thought to have been transferred out of CardSystems' network.
- Visa and MasterCard maintain that notification responsibility falls with the banks that issue credit cards because they have direct relationships with the affected customers.

Vendor Responsibility

- Vendor's must be required to assume at least some responsibility for their mistakes.
- Be proactive. To the extent possible negotiate contract language that defines the notification responsibilities

Questions



Thank You