- **Jan 2008 – Life is Good:** Online Retailer Settles Charges That It Left Consumer Data Open to Hackers. The FTC said a company called "Life is good" lacked "reasonable and appropriate security for the sensitive consumer information stored on its computer network. "Life is good" will use a third-party security auditor to assess its security biennially for the next 20 years and certify that the company meets or exceeds the terms of the FTC settlement.

- **Jan 2008 – EDS**: About 260,000 participants in Medicaid programs were sent a recent mailing that included the recipients' Social Security numbers above their names on the address labels, the state Department of Health and Family Services said …. While 485,000 copies were supposed to go out, the mailing was stopped after a recipient caught the error, according to EDS Corp., the vendor responsible for processing the mailings.

- **Jan 2008 – Sears:** Class Action Suit Alleges Sears Privacy Failures: Class-action lawyers are circling around retailer Sears, Roebuck & Co., just days after privacy activists revealed that the company's Web site exposed the details of customer purchases going back more than a decade…. plaintiffs allege that the lack of privacy protections at Sears's managemyhome.com site violated its own privacy promises to consumers, and in so doing ran afoul of the Illinois Consumer Fraud Act, which prohibits "unfair and deceptive practices."

- **Jan 2008 - Geeks.com:** Notified an unspecified number of customers that their personal and financial data may have been compromised by an intrusion into the systems that run the online technology retailer's Web site. . . The compromised information included the names, addresses, telephone numbers and Visa credit card numbers of an unspecified number of customers who had shopped at Geeks.com.

- **Jan 2008 - RG Cabinets:** A manufacturer of custom cabinets, lost $85,000 in December when computer hackers tapped into their computer system. The hackers increased not only the limits on withdrawals but also withdrew $85,000 in four unauthenticated wire transfers.

- **Dec 2007 - West Penn Allegheny Health System:** Officials are warning of a security breach. Officials said someone stole a laptop computer containing patient data from a homecare nurse's home in November. The breach puts 42,000 patients at risk for identity theft. The laptop, stolen Nov. 24, contained names, birth dates, Social Security numbers, addresses and health care histories of patients in the home care departments of West Penn Hospital, Allegheny General Hospital and Forbes Hospice.

- **Dec 2007 – NY State:** *You are now Liable for Unintentional Medical Data Breach in NY State*: Health care employers be warned -- an unintentional data breach could now cost you much more than you imagined. A New York State Appellate Court has recently upheld a $365,000 jury award against a health care center that mistakenly disclosed information regarding a patient's medical information

- **Dec 2007 – Tricare & EDS:** Letters are in the mail to about 4,700 households who submitted claims through the Tricare Europe office since 2004 about a data breach involving their personal information -- a month after the breach was reported . . .Electronic Data Systems notified Tricare on Nov. 7 that they had not properly secured a part of the system it maintains for Tricare, and "certain external entities" had been allowed access to a file with personal information. That file contained full or partial Social Security numbers. For one or more members of each household, it included their name, date of birth, and a medical diagnosis code associated with a health benefits claim submitted to Tricare Management Activity

- **Dec 2007 – Forrester Research**: Thieves stole a laptop from the home of a Forrester Research employee during the week of Nov. 26, potentially exposing the names, addresses and Social Security numbers of an undisclosed number of current and former employees and directors, the company said in a letter mailed to those affected on Dec. 3..

- **Nov 2007 - Commerce Bank:** is warning some of its customers of a security breach. Their personal information could be in the wrong hands. The bank is warning customers of a possible identity fraud problem. . . important information was breached including: names, addresses, social security numbers and dates of birth, which can all be used to steal people's identities . . .

- **Oct 2007 - Not Your Average Joe's:** A Massachusetts restaurant chain said that thieves have stolen credit card data belonging to its customers. The Dartmouth-based chain estimated less than 3,500 of the 350,000 customers it served in August and September had their credit card information stolen…. Officials at Cape Cod Five Cents Savings Bank reported to local police that a handful of customers were seeing unauthorized charges showing up on their credit card statements.

- **Oct 2007 - Administaff Inc.:** A Houston-based provider of outsourced human resources services, began notifying about 159,000 former and current employees about a stolen laptop containig their unencrypted personal data.

- **Sept 2007 - The Gap:** One of its vendors lost laptops with information on 800,000 job applications. The data had been stored on two laptop computers that were stolen from the vendor's offices. Although the job applicant information on the laptop -- which included Social Security numbers -- was supposed to be encrypted, it was not.

- **Sept 2007 - Accenture:** Connecticut officials today revealed plans to file a civil complaint against IT consulting giant Accenture Ltd. related to a security breach involving stolen records tied to state agency bank accounts worth millions of dollars. State Attorney General Richard Blumenthal said, in a statement about the pending lawsuit, that New York-based Accenture treated the state's confidential information "like scrap paper" and that the company deserves censure.

- **Sept 2007 - Vertical Web Media:** said its network was breached in August and hackers made off with customers' names, addresses, phone numbers and e-mail addresses, along with credit card numbers and expiration dates.

- **Sept 2007 - Unisys:** Blamed in DHS Data Breaches. The FBI is investigating a major information technology firm with a $1.7 billion Department of Homeland Security contract after it allegedly failed to detect cyber break-ins traced to a Chinese-language Web site and then tried to cover up its deficiencies

- **Sept 2007 - ABN Amro Mortgage Group:** Mortgage Data Leaked Over File Network. Three spreadsheets containing more than 5,000 Social Security numbers and other personal details about customers of ABN Amro Mortgage Group were inadvertently leaked over an online file-sharing network by a former employee.

- **Sept 2007 - TD Ameritrade Holding:** The online brokerage manages more than 6.3 million accounts, said unidentified intruders were able to infiltrate a database after they installed a backdoor on the company's computer network. With help of an outside forensic data firm, investigators were able to determine the hackers accessed clients' email addresses, names, addresses, phone numbers and other information, such as the number of trades placed in a given time period.

- **Sept 2007 – ADP:** Says hackers targeted clients in phishing scam. Automatic Data Processing, the payroll processor, said hackers stole business contact information about clients from a third-party database and were now sending bogus and potentially harmful e-mails. ADP said the information taken did not contain social security numbers, bank accounts, passwords or confidential data.

- **Sept 2007 – Pfizer:** revealed its third data breach in three months, this time affecting the personal information of an estimated 34,000 people….. the breach involved the names and Social Security numbers (or Taxpayer Identification numbers) of all people affected. In some cases, it said, home addresses, home and/or cell phone numbers, fax numbers, e-mail addresses, credit card numbers, bank account numbers, passport numbers, driver's license numbers, military identification numbers, birth dates, signatures and reasons for termination of employment were exposed as well

- **Aug 2007 - TradeFreedom Securities Inc:** Online broker TradeFreedom Securities Inc. has quietly notified an unidentified number of its customers that a computer security breach has compromised some of their personal information, potentially exposing them to fraud.

- **Aug 2007 – Pfizer:** Reports Laptops Stolen In 2nd Breach In Two Months. Pfizer criticized earlier this year for a data breach that exposed 17,000 current and former employees to possible identity theft, has notified state Attorney General of the theft in May of two company laptops containing personal information of 950 people.

- **Aug 2007 – VeriSign:** A VeriSign employees laptop was stolen from a car…The laptop contained personal information - name, Social Security number, date of birth, salary information, telephone numbers, and home addresses - of an unknown number of VeriSign employees. Data on the machine was not encrypted, in contravention of VeriSign policies, raising ID theft concerns.

- **July 2007 - Science Applications International Corp:** a government contractor handling sensitive health information for 867,000 U.S. service members and their families acknowledged yesterday that some of its employees sent unencrypted data -- such as medical appointments, treatments and diagnoses -- across the Internet.

- **July 2007 - Disney Movie Club**: An employee who works for a 3rd party company (Alta Resources Inc.) that processes Disney Movie Club transactions was caught trying to sell customer credit card information. The Disney Movie Club has 1 million members, but not all had their data stolen. In some cases, the stolen data included telephone numbers and e-mail addresses.

- **July 2007 - Kingston Technology Company:** A September 2005 security breach that remained undetected until "recently" may have compromised the names, addresses and credit card details of roughly 27,000 online customers of the computer memory vendor.

- **July 2007 – Fidelity:** Admits theft of data on 2.3m customers. Fidelity National Information Service**s** has admitted that personal information on 2.3 million people has been illegally removed from its database. The breach occurred at **Certegy Check Services**, a company that handles cheque and credit card monitoring for merchants and casinos…..

- **June 2007 - Concord Hospital:** Concord Hospital has fired the Washington-based company that it said managed its online billing system and left the personal information of more than 9,000 patients unprotected on the Internet for more than a month. Hospital officials are asking for an audit to verify that Verus Inc. has removed all of its patient information from

its servers. Verus accidentally posted the patients' names, addresses, birthdates and Social Security numbers on the web when a computer security system was disabled for maintenance but never replaced, the hospital said.

- **June 2007 - Pfizer Inc:** Personal data on 17,000 employees exposed… an employee who installed unauthorized file-sharing software on a company laptop provided for use at her home has exposed the Social Security numbers and other personal data belonging to about 17,000 current and former employees at the drug maker.

- **May 2007 - Jax Federal Credit Union:** (Tempe FL) -- has hired a firm specializing in identity theft protection services, to guard 7,766 customers after their personal information, including their social security numbers, was accidentally exposed on Google.

- **May 2007 - Sky Bank:** (INDIANAPOLIS) -- A security breach has left some customers vulnerable to hackers as Sky Bank officials confirmed a problem with some debit cards.

- **May 2007 - Columbia Bank:** hacked, notifies users of ID theft. Hacker outside the bank gained access to customers' names and Social Security numbers, and "the intrusion affected all of our customers who have online banking,"…… Columbia Bank is offering one year of free credit-monitoring services for affected individuals. Grayson Barber, a Princeton lawyer and privacy-rights advocate who sat on the state's Privacy Rights Commission, said a year is not enough.

- **May 2007 – J.P. Morgan:** claims by a Washington D.C.-based workers union that JPM dumped documents containing personal financial data belonging to its customers in garbage bags outside five branch offices in New York. Separately, it is also sending out letters to tens of thousands of Chicago-area customers and some employees about the potential compromise of their account information after a tape containing the data was reported missing.

- **April 2007 - Ceridian:** Data from NY firm accidentally leaked; Payroll processing firm Ceridian Corp. said employee data from a New York advertising firm had been accidentally leaked on a Web site, the company confirmed.

- **April 2007 - Neiman Marcus:** Computer equipment containing the personal data of nearly 160,000 current and former employees of the Neiman Marcus Group Inc. has been stolen, the high-end retailer. The equipment is owned by a third-party pension benefits plan consultant that has not been named. The stolen files contain data from 2005, including Social Security numbers and salary information.

- **April 2007 - Tuscaloosa-based Hospital:** loses personal data on employees. Social Security numbers and other personal data on more than 6,000 employees and retirees of DCH Health System are missing after a consulting company lost a computer disk and documents containing the information.

- **Jan 2007 – TJX:** Disclosed that "unauthorized intruder" gained access to its systems in mid-December and may have made off with the card data of customers in the U.S., Canada and Puerto Rico, as well as the U.K. and Ireland. It was reveled 46 Million customers may have been impacted. This has resulted in several class action approaching 1 Bill in alleged damages.

- **Jan 2007 - Nationwide Health Insurance:** The personal information of more than 28,000 Nationwide Health Plans customers has been stolen including medical-claim data, health information and Social Security numbers.

- **Jan – 2007: MoneyGram International Inc:** a global payment services provider, announced that a company server with consumer information for about 79,000 bill payment customers was unlawfully accessed over the Internet last month.

- **Dec 2006 - University of Texas at Dallas:** discovered over the weekend that social security numbers and other sensitive information relating to 5,000 students, faculty members and staff may have been exposed by a computer network intrusion. Phone numbers, e-mail addresses and home addresses also may have been exposed.

- **Dec 2006 – UCLA:** major security breach at UCLA after a hacker broke into the campus computer system. University officials are alerting about 800,000 current and former students, faculty and staff today. The database includes social security numbers, home addresses and birth dates.

- **Nov 2006 - Starbucks Corp:** said it had lost track of four laptop computers, two of which had private information on about 60,000 current and former U.S. employees and fewer than 80 Canadian workers and contractors.

- **Nov 2006 - Affiliated Computer Services:** A computer stolen from ACS holds a database that may contain personal information of up to 1.4 million Coloradans. ACS's $5.5 million contract with the state, which it has had since 1999, won't be renewed when it ends next year.

- **Nov 2006 - Sisters of St. Francis Health Services:** An Indiana man has sued the hospital system over a security lapse that might have exposed the private information of more than 260,000 patients. Claims in a federal lawsuit the hospital violated federal HIPAA privacy laws and failed "to take reasonable corrective action" such as promptly notifying patients of the breach. It seeks damages, including no less than $5,000 for each affected class member

- **Oct 2006 - Akron Children's Hospital:** notifying about 230,000 patients that someone hacked into its computer system and gained access to sensitive information, including Social Security numbers and bank account records. The computer breach happened over Labor Day weekend, but the hospital didn't alert the FBI until last week. It didn't start notifying patients until this week.

- **Sept 2006 – Second Life Game site**: Online fantasy game site "Second Life" has suffered a security breach in which the data of 650,000 users may have been exposed, including real names, addresses and billing information. A security alert on the game's site noted that encrypted payment information and passwords were potentially exposed, and that users should change their passwords.

- **Sept 2006 - Xanga.com:** settles child privacy lawsuit. FTC announced a $1 million settlement with the social networking site Xanga.com, the largest penalty levied to date under the Children Online Privacy Protection Act. The complaint charges that the defendants knew they were collecting and disclosing personal information from children. Over the past five years, the site allowed 1.7 million visitors to create Xanga accounts after they provided a birth date indicating they were under that age.

- **Aug 2006 - Valley Baptist Medical Center:** A computer glitch on a hospital web site left some people at risk for identity theft. Names, birth dates, and social security numbers of various healthcare workers - potential 73 victims - that were posted on Valley Baptist Medical Center's web site late last week

- **Aug 2006 – AT&T:** Hackers illegally accessed a computer system and stole credit card information and other personal data from thousands of customers who purchased DSL equipment from an AT&T online store. AT&T Inc. said the system was hacked into over the weekend. The data of "fewer than 19,000 customers" was affected.

- **Aug 2006 – AFLAC:** Insurance giant that a laptop computer containing personal information on hundreds of customers was stolen from an agent's car in the Greenville area. The computer contained names, addresses, Social Security numbers and birth dates of 612 policy holders. The information is protected by a password. Also, the computer is equipped with tracking software that will alert officials when the computer is connected to the Internet.

- **Aug 2006 – AOL:** Two AOL employees were fired and its chief technology officer has left the company in the aftermath of a privacy breach that involved the intentional release of more than 650,000 subscribers' Internet search terms. Although AOL had substituted numeric IDs for the subscribers' user names, the search queries themselves contained Social Security numbers, medical conditions and other data that could be traced to an individual.

- **August 2006 - BAE Systems**: BAE Systems National Security Solutions Inc. on Aug. 2 notified 4,500 current and former employees, retirees and consultants that a Trojan virus had been found on a company computer server…..July 18, the company discovered someone obtained unauthorized access to a company computer server at its main office in San Diego, Calif……The server contained the names, addresses Social Security numbers, birth dates, telephone numbers, maiden names and personal vehicle information, according to the letter.

- **August 2006 - Sentry Insurance:** The property, casualty and life insurance provider for personal and commercial customers, reported today that personal information on more than 112,000 of its customers was stolen, and that data on 72 of them was sold over the Internet. The data sold over the Internet included people's names and Social Security numbers but not medical records, Sentry said. All victims were involved with workers' compensation claims.

- **June 2006 – WIU:** A recent intrusion into Western Illinois University's computer system has forced school officials to notify students and alumni that their data could have been compromised. While university officials do not believe any records were copied from the system, data from anywhere between 200,000 and 240,000 students and alumni may have been compromised

- **June 2006 – AIG Corp:** A thief recently stole a computer server belonging to AIG major U.S. insurance company, and company officials now fear that the personal data of nearly 1 million people could be at risk. The computer server contains personal electronic data for 930,000 Americans, including names, Social Security numbers and tens of thousands of medical records. The server was stolen on March 31 during a break-in at a Midwest office of AIG company officials confirm.

- **June 2006 – PaineWebber:** Systems Admin Faces Trial For Computer Sabotage. Former employee charged with building and planting malicious code that took down two-thirds of the company's network, hindering investment trading for several weeks and racking up $3 million in recovery costs.

- **June 2006 - Ernst & Young:** E&Y laptop loss exposes 243,000 Hotels.com customers

- **June 2006 – EDS:** loses personal data on Tops Markets (supermarket chain) retirees, ex-employees: The vendor, EDS, provides data processing services for the Ahold USA pension

plan. An employee lost a laptop with the personal data in early May during a flight between Philadelphia and Boston, said Texas-based EDS.

- **May 2006 – Hospital DDoS Outage**: A U.S. man has pleaded guilty of creating a zombie network of 50,000 computers to launch a devastating attack against Seattle's Northwest Hospital. The attack is said to have shut down computers in the facility's intensive care unit and prevented doctors' pagers from working properly

- **May 2006 – Ohio State:** Hackers strike OU alumni database: 137,000 Social Security numbers has been exposed; separate data theft also under investigation

- **April 2006 - University of Southern California:** The DOJ said in a statement yesterday that a hacker exploited a vulnerability in the admissions structured query language (SQL) database to bypass authentication. He staged a SQL injection with the same Gmail account, and accessed and copied several applicant records. Though he only accessed a small number of records, the breach compromised more than 270,000 records housed in the database.

- **April 2006 - University of Alaska Fairbanks:** University officials say the hacker had access to the names, Social Security numbers and partial e-mail addresses of nearly 39, 000 current and former University of Alaska Fairbanks students, faculty and staff

- **April 2006 - University of Texas:** As many as 197,000 individuals associated with the University of Texas McCombs School of Business may have had personal information stolen from the school's computers. The information includes first and last names, dates of birth, zip codes and Social Security numbers. No class schedule, transcripts or grade information was involved

- **February 2006 – OfficeMax:** The California retailer at the heart of a major data-security breach affecting as many as 200,000 consumers, banking and law-enforcement sources confirmed. They also said investigators are exploring the possibility that the Russian mob or another Eastern European crime syndicate is responsible for accessing U.S. consumers' debit-card numbers and selling counterfeit cards on the black market worldwide.

- **February 2006 - Russian Stock Market:** The denial-of-service caused the Russian Trading System (RTS) to stop trading for over an hour. It appears that a hacker gained access to a local machine connected to the network of the RTS, and then launched the DoS attack.

- **February 2006 - Providence Health System:** A Portland woman has sued the Providence Health System claiming it put patients at risk of identity theft when private records of 365-thousand patients were stolen from an employee's car. It asks for an immediate court order making Providence pay for ongoing credit monitoring for theft victims and to pay for restoring potential damage to credit ratings

- **February 2006 - UCCS:** Personal information on about 2,500 current and former employees at the University of Colorado at Colorado Springs has been compromised by someone who hacked into a computer and infected it with a virus. Names, Social Security numbers, birth dates and addresses for employees dating back to 2004 were accessed without authorization.

- **February 2006- Honeywell International:** acknowledged late Tuesday that personal information, including Social Security and bank account numbers, on 19,000 employees was inadvertently posted to a public Web site

- **January 2006 - New York Times-owned papers:** say they may have exposed 240,000 subscribers' information. the *Boston Globe* and *Worcester Telegram & Gazette*, said Tuesday they had mistakenly sent out slips of paper with the credit card data of up to nearly a quarter million subscribers.

- **January 2006 - ChoicePoint:** The FTC announced ChoicePoint Inc. will pay $15 million to settle charges that its security and record-handling procedures violated consumers' privacy rights and federal laws. The settlement requires ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program and to obtain audits by an independent third-party security professional every other year until 2026.

- **January 2006 – Notre Dame:** Hacker causes Notre Dame's first significant computer security intrusion. The personal and financial information of some University donors may be at risk after an unknown intruder hacked into a Development Office server Jan. 13 - the first computer security breach of its magnitude at Notre Dame, University

- **January 2006 – PNC Bank:** A "very small number" (2000) of PNC Bank's credit and debit-card accounts were compromised by suspicious activity that originated overseas, triggering cancellations and the issuance of new cards.

- **January 2006 - Atlantis Data Breach:** Bahamas luxury resort Atlantis Data Breach reported to the SEC they had information lifted from their computer system with some 55,000 identities compromised. It appears this is a pretty standard identity theft. The information stolen included names, addresses, social security numbers, drivers' license numbers, credit card and bank account information.

- **January 2006 - Y-12 Federal Credit Union:** Hackers tap Y-12 credit union accounts through software breach. Hackers broke into a Tennessee credit union's Web site, lured online customers to a bogus site in Greece and then snatched their credit card numbers and personal identification numbers or PINs. Within hours, the Visa accounts of 30 customers of the Y-12 Federal Credit Union in Oak Ridge were tapped for more than $70,000 through ATM withdrawals

- **December 2, 2005 - University of San Diego:** Hacker Breaks Into USD Computers: About 8,000 students, faculty, staff and vendors who were at the University of San Diego, or did business with the university, between 2003 and 2004 are being warned their personal information may have been taken by hackers.

- **11/30/05 - University of Delaware:** Two recent security breaches of computers at the University of Delaware. The computer contained a database that included Social Security numbers of 772 students registered in online education courses.

- **11/30/05 - Scottrade:** Hacker imperils data of 140,000 Scottrade clients. An Internet hacker might have gained access to personal and financial data of about 140,000 customers of Scottrade Inc., a stock brokerage based in St. Louis County..... Possible exposed information included names, birth dates, drivers license numbers, phone numbers, bank names, bank routing numbers, bank account numbers and Scottrade account numbers.

- **9/29/05: University of Georgia:** Computer breach reported at UGA. A hacker broke into a computer database at the University of Georgia, gaining access to the Social Security numbers of employees in the College of Agricultural and Environmental Sciences and people who are paid from that department. More than 2,400 numbers, belonging to roughly 1,600 people, may have been exposed.

- **Sept. 27 2005 - City University of New York:** blamed human error for making sensitive financial information for 300 law school students public on the Web. "It's a human error ... that placed the file outside a protected firewall,"

- **Sept 2005 - Miami University (OH):** suffered a computer security breach, which involves 21,762 students on all of the university's campuses. This was discovered after a Miami graduate alerted the alumni office.

- **August 8 2005 - Sonoma State University:** announced that personal information of more than 61,000 students who applied or attended the university between 1995 and 2002 were accessed during a July hacker attack.

- **August 2 2005 - The University of Colorado at Boulder:** said 29,000 students and 7,000 staff were vulnerable to identity theft from a hacker attack -- the third in two weeks.

- **August 2005 - University of North Texas:** server was discovered to have been breached, affecting nearly 39,000 students.

- **June 20, 2005 - CardSystems Solutions Inc:** A computer-security breach at a company that processes credit-card transactions exposed more than 40 million cards of all brands to possible fraud, laying bare the vulnerability of obscure nooks of the nation's sprawling electronic-payments system.

- **May 2005 - Duke University Health System:** websites to access potentially sensitive information last May. The DUHS website attack compromised 5,500 users' passwords and more than 8,000 fragments of social security numbers.

- **May 25, 2005: University of Cincinnati** said a hacker got into the school's computer system last month and they're still trying to determine what all he or she was able to see. Other evidence continues to pop up as the staff continues to research mountains of data from UC's 400 servers. A hole in the computer security system has been patched.

- **May 25, 2005 - Purdue University:** About 679 Indiana University-Purdue University Fort Wayne employees could be victims after a hacker tapped into a Purdue University computer network. The program contained university credit card information and the Social Security numbers of employees, and retired and former employees.

- **May 25, 2005 – Brigham Young University:** More than 600 BYU students may be the victims of a computer hacker. School officials detected a program in one of the computer labs on campus that recorded students' keystrokes.

- **May 20. 2005 - Westborough Bank**: The bank warned customers that a former bank employee may have provided Christos Kyriazis, 41, of St. Petersburg, Fla., with personal information taken from bank records without authorization. Kyriazis was arrested last month for allegedly defrauding an elderly Shrewsbury woman of nearly $1 million over a three-year period beginning in 2001

- **May 11, 2005 - Stanford University:** The FBI is investigating a computer system security breach at Stanford University that may have put the personal information of nearly 10,000 people at risk. Client records included Social Security numbers and resumes, financial or government information.

- **May 2005 - Bank of America, Wachovia, PNC Bank and Commerce Bancorp:** Police say that a New Jersey man was running a ring of "upper-level" bank officials who were bribed to provide data on customers. The data subsequently was sold to dozens of debt collectors and law firms. The event involves more than 670,000 customers at four different banks. The U.S. Treasury Department is calling it the largest financial security breach in history.

- **April 2005 - Ralph Lauren:** Polo Ralph Lauren Corp. blamed a software glitch for a security breach that prompted HSBC North America to notify 108,000 holders of its General Motors-branded MasterCard that their personal information may have been stolen.

- **April 2005 - DSW Shoe Warehouse:** Retail Ventures Inc. this month reported that personal customer information from 108 stores in its DSW Shoe Warehouse subsidiary was stolen. The information, involving 1.4 million credit cards used to make purchases mostly between November and February, included account numbers, names, and transaction amounts.

- **April 22, 2005 - Carnegie Mellon University:** Officials advised someone hacked into their computer system -- potentially gaining access to the personal information of 6000+ students, alumni and employees. They had access to social security numbers, credit card accounts and other sensitive personal data.

- **April 12, 2005 – Tufts University:** Tufts last week began sending letters to **106,000 graduates**, warning of ``abnormal activity'' on a computer that contained names, addresses, phone numbers, Social Security and credit card numbers.

- **March 29, 2005 – UC Berkley:** The University of California, Berkeley, is the latest institution of higher leaning to report a computer security breach where the sensitive personal data of tens of thousands of people may have been compromised. A laptop was stolen containing the information of more than 98,000 people from a graduate school admissions office, the university said in a statement released on its Web site.

- **March 28 2005 - The San Jose Medical Group:** notified about 185,000 people that they are at risk for identity theft after burglars stole two Dell computers from the group's administrative offices March 28. The computers contained patient names, confidential medical information, and Social Security numbers.

- **March 2005 – Cal State Chico**: Hackers broke into California State University, Chico's housing and food service computer system, which contained vital information about 59,000 current, former and prospective students, as well as faculty and staff.

- **March 11 2005, Boston College** officials warned 120,000 alumni that their personal information may have been stolen when an intruder hacked into a school computer containing the addresses and Social Security numbers of BC graduates.

- **March 9, 2005 – LexisNexis:** estimates that information on 310,000 U.S. individuals may have been accessed. When it first reported the thefts March 9, the company said about one-third of the victims were California residents

- **March 2005 - Bank of America:** lost computer data tapes with encrypted account information on 1.2 million federal employees.

- **Feb 21 2005 - Choicepoint**: ChoicePoint (CPS), a personal-information clearinghouse, is notifying almost 145,000 people nationwide that their data - including credit reports and

Social Security numbers - may have been stolen from the company's database. California authorities say 500,000 people could be affected.

- **Feb 4 2005 - Indiana University:** FBI probes IU computer hacker. BLOOMINGTON, Ind. -- The FBI and campus police are investigating a computer security breach at the Indiana University Foundation that left employees' personal information vulnerable.

- **January 21, 2005 – Harvard:** Harvard ID numbers, PharmaCare loophole provide wide-ranging access to private data.

- **Jan 2005 - T-Mobile:** The T-Mobile network was penetrated and the attacker obtained customer personal data. **16.3 million customers** were impacted, including many customers' Social Security numbers and dates of birth, according to government filings in the case.

- **Jan 2005: George Mason University** : Computer hackers captured the names, Social Security numbers and other information of more than **30,000 students** and staff at George Mason University

- **Dec 2004 - McDonalds:** Hacker Hits McDonald's China Web Site Over Taiwan

- **June 2004 - AOL:** An AOL insider sold to spammer a list of AOL user screen names, ZIP codes, phone numbers and credit card types (not numbers) of 92 million e-mail addresses for AOL's 30 million customers

- **June 2004 - Survey - 2 million bank accounts robbed:** Nearly 2 million Americans have had their checking accounts raided by criminals in the past 12 months, according to a soon-to-be released survey by market research group Gartner. Consumers reported an average loss per incident of $1,200, pushing total losses higher than $2 billion for the year.

- **May 16 2004 – Ciscso:** Cisco Source Code Reportedly Stolen. **C**riminal hackers broke into Cisco's corporate network and stole 800MB of source code for IOS 12.3 and 12.3t (an early deployment version containing features not found in the vanilla 12.3 version). If the report is accurate, this represents a major security threat not just for Cisco users, but for the entire Internet.

- **May 6, 2004 - University of California San Diego:** Hacker Accesses UCSD Computers. SAN DIEGO -- About 380,000 University of California San Diego students, alumni, applicants, staff and faculty are being warned that a hacker may have had access to their personal information.

- **April 30, 2004 – Barnes & Noble:** Barnes & Noble.com Fined for Customer Data Leak. New York-based online bookseller Barnes & Noble.com has been slapped with a $60,000 fine after a flaw exposed sensitive customer data on its Web site.

- **Tower Records:** settles government charges over hacker attacks. WASHINGTON -- The company that operates the Web site for music retailer Tower Records has settled complaints by U.S. regulators that it allowed hackers in 2002 to steal personal information about thousands of its online customers.

- **Indiana State University:** Hacker Breaks Into ISU Computer. Indiana State University officials say a hacker broke into a computer Server containing personal information of about 35-thousand current and former students and staff

- **Internet Technology Vulnerable to Hackers**: WASHINGTON - Researchers uncovered a serious flaw in the underlying technology for nearly all Internet traffic, a discovery that led to an urgent and secretive international effort to prevent global disruptions of Web surfing, e-mails and instant messages.

- **3/12/04 - BJ's Wholesale:** consumer info may have been stolen. DENVER, March 12 (Reuters) - BJ's Wholesale Club Inc. (BJ) said on Friday its computer system may have been compromised and it has alerted its members that their credit card information may have been stolen. The Natick, Massachusetts, warehouse club operator said in a statement it recently learned that a small fraction of its 8 million members may have been affected.

- **4/7/04 – Kansas University:** Hacker accesses KU files. The Personal information of thousands of Kansas University students, faculty and staff may have been taken by a computer hacker last week, KU officials said.

- **Microsoft Grapples With Source Code Leak:** SEATTLE - Microsoft Corp. says incomplete portions of the source code for some versions of its Windows computer operating system were leaked over the Internet. Access to the source code could allow hackers to exploit the operating system and attack machines running some versions of Windows. Several versions of the operating system, including the ones containing leaked code, are used on hundreds of millions of computers worldwide.

- **University of Georgia:** Officials Investigate Hack at U. of Ga. ATHENS, Ga. - Federal and state authorities are investigating whether hackers gained access to Social Security and credit card numbers of 31,000 University of Georgia students and applicants, officials said.

- **Georgia Tech:** Hackers strike Georgia Tech computer, gain credit card data. Computer hackers invaded a computer at Georgia Tech and copied names, addresses and -- in some cases -- credit card information for 57,000 patrons of the Ferst Center for the Arts.

- **3/6/03 – University of Texas:** Hackers steal names, Social Security numbers from University of Texas database. Austin -- Hackers broke into a University of Texas database and stole the names, Social Security numbers and e-mail addresses of more than 55,000 students, former students and employees, officials said.

- **February 24, 2003 - DPI System**: break-in nets hackers 8 million credit card numbers. A credit card transaction processing company last week confirmed that millions of card numbers were stolen recently when someone hacked into its computers. But it defended itself by saying the culprits may not have obtained any useful information. Omaha-based Data Processors International Inc. (DPI) acknowledged in a statement that it "experienced a system intrusion" four weeks ago.

BSR
PO Box 768 · Hendersonville, TN 37075
(T) 800-768-7475 · (F) 615-264-3980
www.bsrins.com