2009 REPORT ON DATA BREACH NOTIFICATIONS

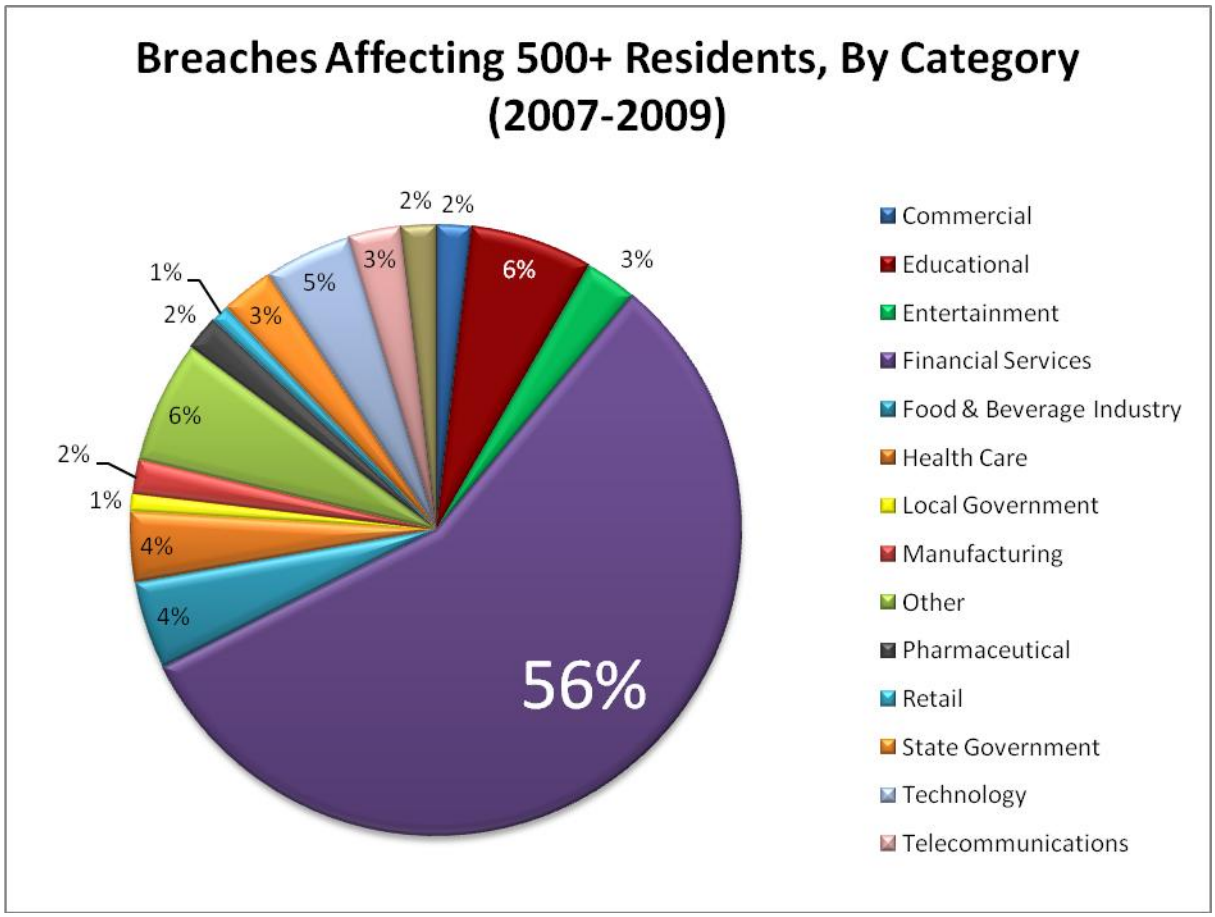
It has now been two years since the Commonwealth's Security Breach law, M.G.L. c. 93H, took effect. Under this law, businesses and others who own or license personal information of Massachusetts residents must, among other requirements, notify the Office of Consumer Affairs and Business Regulation and the Office of the Attorney General when they know of or have reason to know of a breach of security, or when they know of or have reason to know that the personal information of a Massachusetts resident was acquired or used by an unauthorized person, or used for an unauthorized purpose.

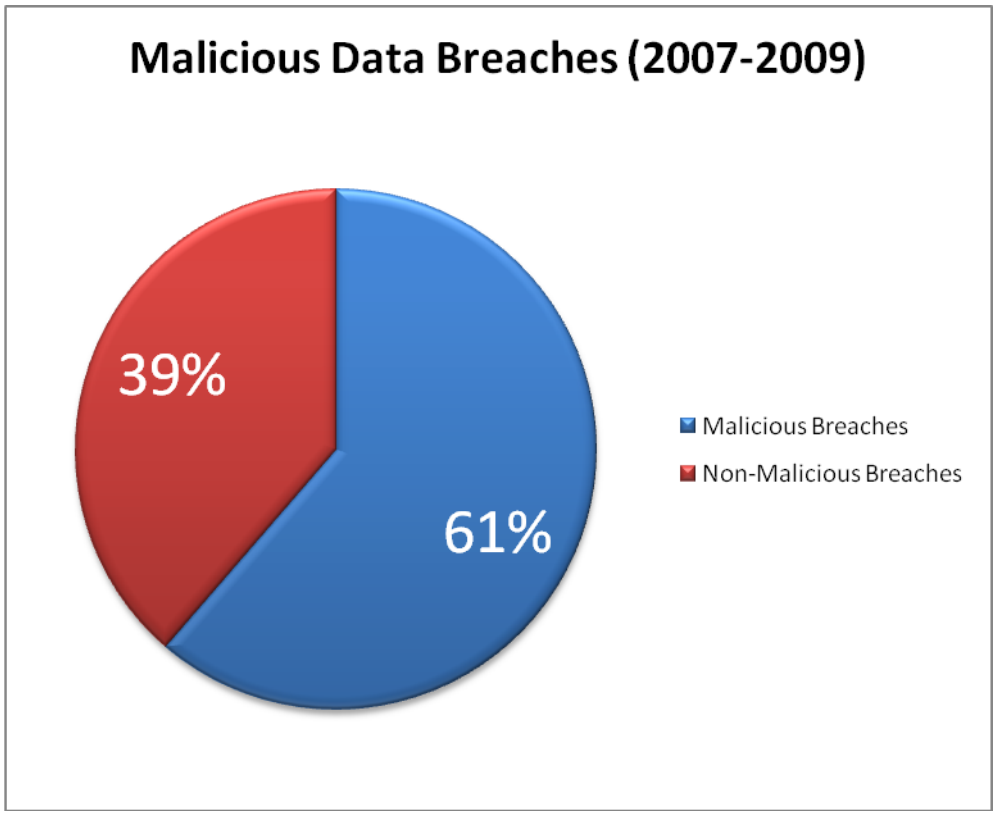
"Personal information" is specifically defined under the law to be: a resident's first name and last name, or first initial and last name, in combination with any one or more of the resident's: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to the resident's financial account. The law provides, however, that "personal information" does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Since the law went into effect, on October 31, 2007, the Office of Consumer Affairs and Business Regulation has received 807 notifications of security breaches. Of those 807 incidents, 746 were reported by businesses, 39 were reported by educational institutions, and 45 were reported by state government. The number of Massachusetts residents affected by the reported incidents is now 1,057,560.

Trends in the reported data show a combination of criminal acts and poor data management practices in security breaches, along with some errors in processing information. The notifications indicated that in 495 cases, the breaches were the result of criminal or otherwise unauthorized acts, including the theft of laptops, outside intrusion into databases that may not have been protected by encryption, or the intentional accessing of information by unapproved individuals. The remaining breach notifications, 312 affecting 522,979 Massachusetts residents, generally demonstrated poor employee handling of residents' personal information, including transporting sensitive data, either in disregard of company policies, or in an environment without sufficient policies in place to secure such information. Some breaches also resulted from the simple act of putting the wrong document into the wrong envelope, or sending attached files to incorrect e-mail recipients.

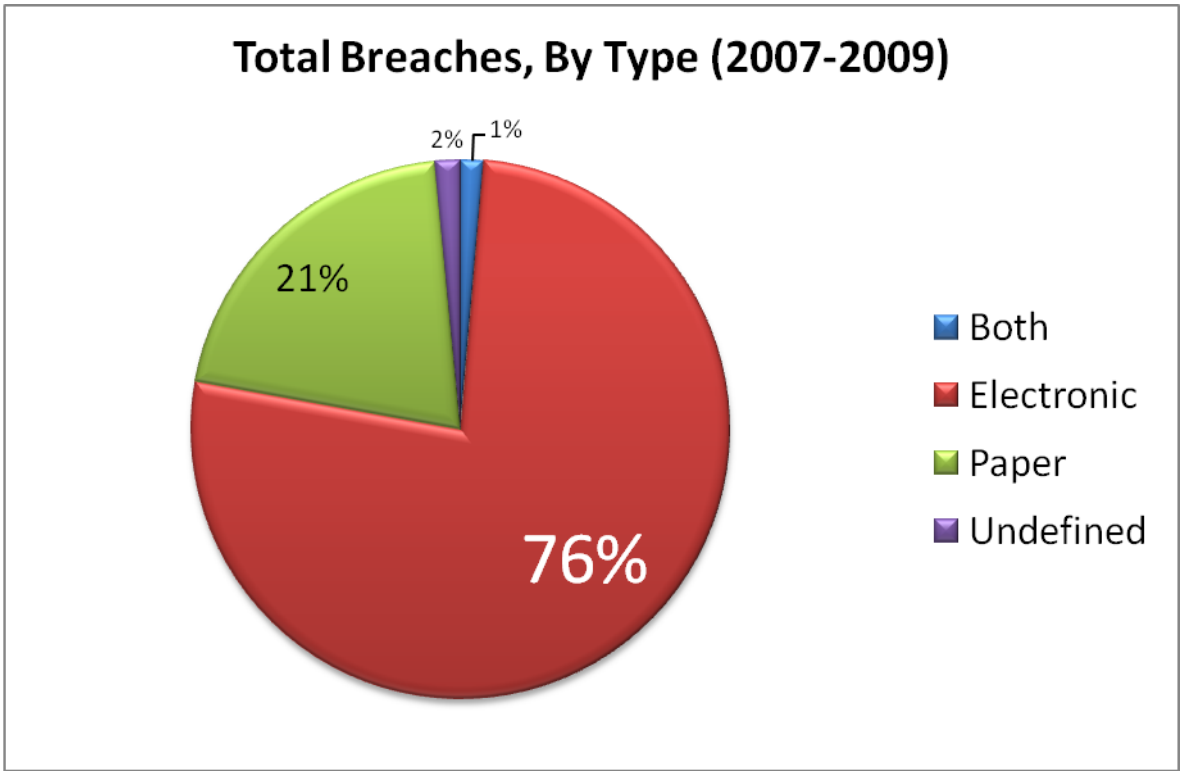
The 108 entities that reported breaches affecting 500 or more Massachusetts residents represented the following categories:



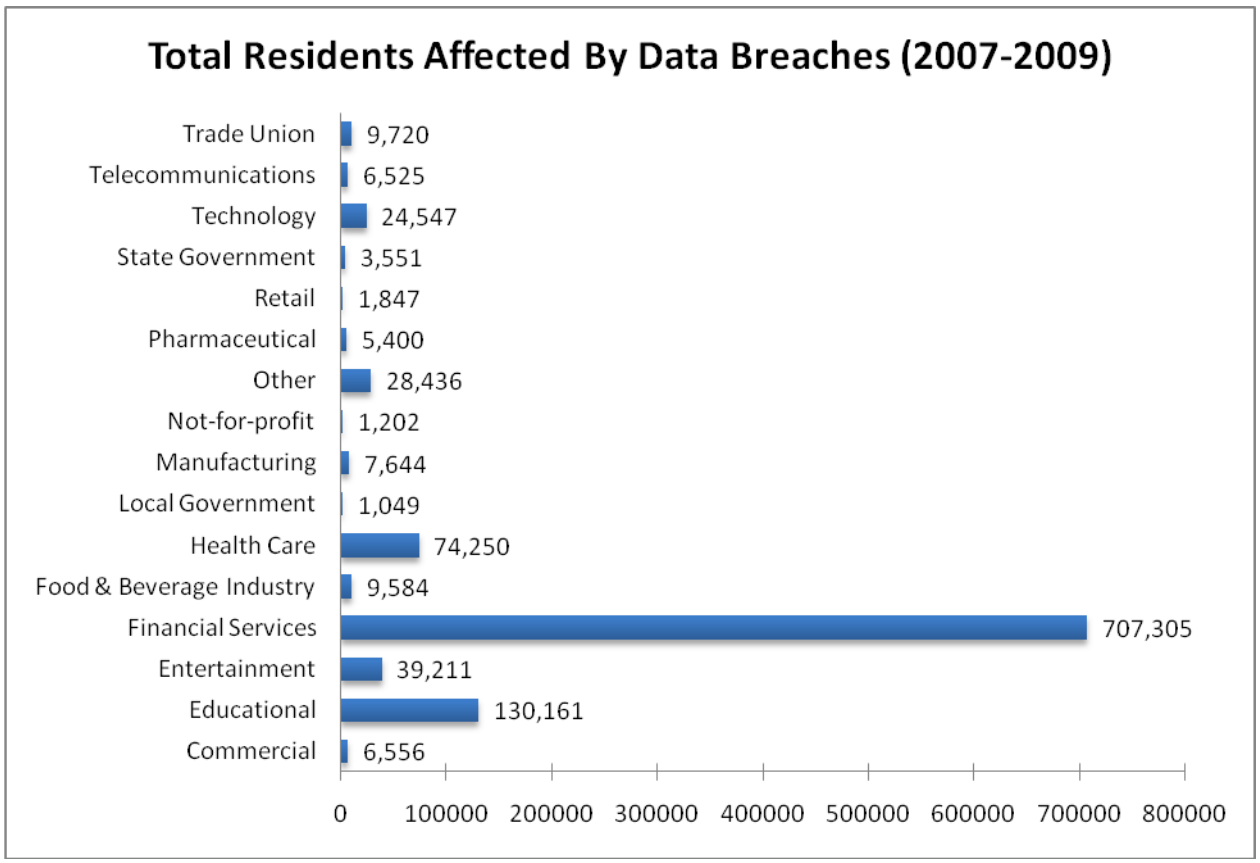


Some of the largest reported breaches involved intentional, unauthorized intrusions into electronic databases. Hacking computer systems and/or placing "malware" which diverted personal information into an unauthorized location appears to have played an increasing role in the loss of personal information. Also in this category were instances of breaches involving former employees whose access rights were not terminated appropriately. Encrypting, and/or purging personal information that it is no longer necessary to maintain, along with immediately terminating access to information as employees leave the work force, could act to limit such losses in the future.

Less dramatic, as it affected fewer individuals at a time, is the unintentional release of personal information by misdirected mailings, inadvertent disclosure to third parties, or other employee mistakes that could have been prevented. If the employees at fault for these breaches had been provided with written policies alerting them to the value of the personal information to the criminal community, and their own obligation to safeguard that information, as well as subject to policies limiting access to those with a need to use the information, it is likely that these breaches would have been fewer in number.



The majority of reported security breaches involve the loss of electronic information, rather than the loss of paper files. 626 of the total reported breaches, affecting 1,0491,126 Massachusetts residents, concerned the loss of electronic files of personal information. While years ago information was maintained in paper files, stored in warehouses or buried deep in vaults and filing drawers in many locations, with the advent of technology and a paperless society, the danger of disclosure or loss of information—and its instant transmission through the internet—cautions that steps should be taken not only to limit access to this information to those persons who need to see it, but also to encrypt and secure the information so that it cannot be transmitted by unauthorized persons and read without the confidential process or key that encryption requires for access.



The reported data also implies that there is information that is not being reported to the Office of Consumer Affairs, either because the affected entity remains unaware that it is subject to the law or for other reasons. Notifications filed by parties that maintain or store information indicate that the financial services sector is the source of risk for 67% percent of data security breaches affecting Massachusetts residents. However, the financial services sector itself may not be notifying the Office of the breaches, as there is not always a corresponding notice from the affected financial institution for some of these otherwise identified breaches.

Building upon its knowledge from these and earlier reported security breaches and in conformance with the requirements of the security breach statute, the Office of Consumer Affairs and Business Regulation has promulgated 201 CMR 17.00, "Standards for the Protection of Personal Information of Residents of the Commonwealth." The regulation will go into effect on March 1, 2010. The regulation implements the provisions of M.G.L. c. 93H, relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth, and it establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. It is anticipated that as businesses and others create and implement the comprehensive written information security programs in conformance with the law and the Office's regulation, the incidence of security breaches caused by unintentional but careless practices will decrease, as will the potential damage to residents whose information is gathered by unauthorized persons, since their information will be guarded by more robust protections, including encryption of information.