COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION
10 Park Plaza – Suite 5170, Boston MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

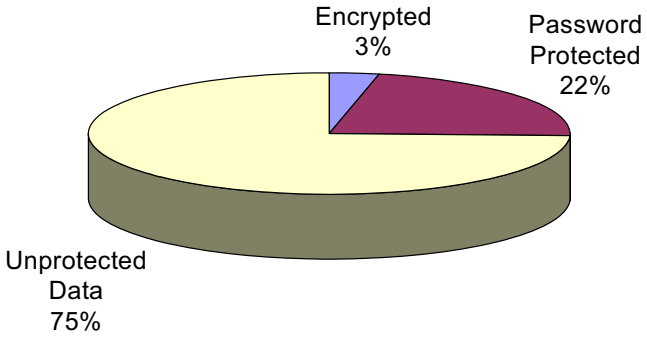
DANIEL O'CONNELL
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

DANIEL C. CRANE
UNDERSECRETARY

REPORT ON THE M.G.L. CHAPTER 93H NOTIFICATIONS

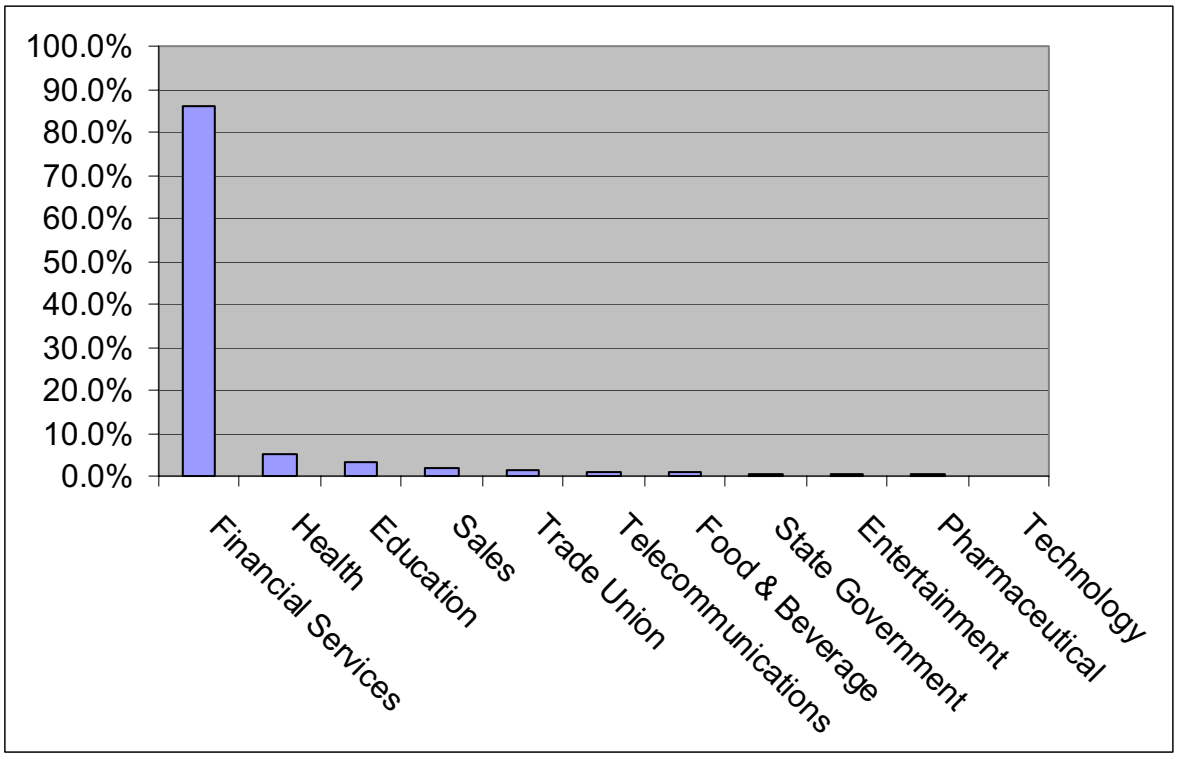
It has now been over 10 months since the new identity theft law took effect. Under that law, businesses and others who maintain and store the personal information of Massachusetts residents must notify the Office of Consumer Affairs and Business Regulation, and the Attorney General, whenever security breaches occur that involve either personal information or unencrypted data capable of compromising personal information in a manner that creates a substantial risk of identity theft or fraud.

During that time, the Office of Consumer Affairs and business Regulation has received 318 notifications of such breaches. Of those 318 incidents, 274 were reported by businesses; 23 by educational institutions; 17 by state government; and 4 by not-for-profits. Of the 318 notifications, only 10 involved data that was encrypted when breached. There were 69 reported incidents of data breach in which the data was password protected.



The number of Massachusetts residents affected by these reported incidents was 625,365. The notifications reported that in 194 cases the breach was the result of criminal/unauthorized acts, with a high frequency of laptops or hard-drives being stolen. Thus, of the remainder of these breaches, approximately 40% of the total, are the result of employee error or sloppy internal handling of personal information or other data. This confirms that any regulatory regime must include both measures that protect against intentional wrongdoing and measures that focus on establishing internal protocols that set minimum standards for handling sensitive paper and electronic records.

The 33 entities that reported breaches affecting more than 500 Massachusetts residents represented the following industries:



While it may be that we have not received notification with respect to every breach that is reportable under M.G.L. c. 93H, §3 (whether because some are not aware of the obligation, or for other reasons have decided not to report a breach), these results suggest that the source of risk for a substantial majority of the Massachusetts residents who are affected by data security breaches (almost 75%) was the financial services sector. The remaining 25% is distributed among other institutions and industries.

The notifications also strongly suggest that the most frequent type of breach was the result of criminal/deliberate acts, mostly thefts and businesses reporting that they had reason to believe that there had been unauthorized access or use of data (though frequently the details of such access or use was not known). The 194 such cases represent more than 60% of the reported incidents.

The need both for expanded use of encryption and for tighter control over third party service providers is illustrated by the BNY Mellon breach affecting 411,547 Massachusetts residents. There, tapes containing personal information of Massachusetts residents were lost in unspecified circumstances by a Mellon service provider. The data on those tapes were reported to have been unencrypted. Both tighter controls on transportation protocols, and the encryption of the information on the mislaid tapes, would have either prevented the loss in the first place, and if not, the loss would have been rendered harmless had the data been encrypted.

The Hannaford loss is similarly instructive. There, new and sophisticated malware installed on company servers intercepted unencrypted data containing 4.2 million credit card numbers and expiration dates that were in transit for authorization from the point of sale. The company reported that none of these data was associated with any address, last name, SSN or driver's license number, and that the company itself did not know the names and addresses of the customers whose card numbers were intercepted. Hannaford had been certified as PCI (Payment Card Industry Data Security Standards) compliant in 2007 and in February, 2008, at the very time, we are told, that the malware interception was taking place! While reasonably up-to-date malware protection might not have been effective against the new and sophisticated malware used in the Hannaford case, encryption of the data would probably have rendered its interception harmless.

The Hannaford breach also illustrated that, in spite of the very limited information intercepted (not actually amounting to personal information as defined in the statute), it was sufficient to launch the next phase of a criminal enterprise. HSBC Retail Services reported to us at the end of April of this year that:

> HSBC recently discovered irregular activity on the Forgot Login Password page of one of our websites, which was caused by unauthorized third parties using scripting that would allow them to view account information after providing the account numbers and the last four digits of the customer Social Security number. HSBC further confirmed that the accounts involved in this security incident has a 95 percent match rate with the accounts

compromised by the third party Hannaford Brothers breach, which was announced to the industry by a recent MasterCard alert.

Thus, the Hannaford incident, coupled with the irregular activity noticed by HSBC, also illustrates why notification of breaches of any unencrypted data (even if it is not personal information) that is capable of compromising personal information, so as to create a substantial risk of identity theft or fraud, is an important part of the consumer protections embodied in the Chapter 93H.

Conclusions

- Notifications from the financial services/insurance industry account for 75% of the total number of Massachusetts residents affected by reported breaches.
- While criminal/intentional unauthorized acts present the major threat to electronic information, employee error and sloppy internal handling of that information are substantial causes of security breaches.
- Almost 75% of the reported incidents appear to have involved data that was neither encrypted nor password protected.
- The Hannaford incident suggests that the Payment Card Industry Data Security Standards are not an effective standard in light of the need for encryption.
- The Mellon incident suggests the need for tighter control over third party providers.
- The Hannaford breach (as understood in light of the HSBC notification) illustrates that data breaches not amounting to the breach of "personal information" have the potential to be as damaging as those that do involve such information.