



THE COMMONWEALTH OF MASSACHUSETTS  
OFFICE OF THE ATTORNEY GENERAL

ONE ASHBURTON PLACE  
BOSTON, MASSACHUSETTS 02108

MARTHA COAKLEY  
ATTORNEY GENERAL

(617) 727-2200  
www.mass.gov/ago

April 8, 2011

Gary Sanford  
Disc Interchange Service Company  
15 Stony Brook Road  
Westford, MA 01886

Dear Mr. Sanford:

I write in response to your letter of March 17, 2011. Your letter concerned 210 CMR 17.00 *et seq.*: Standards for the Protection of Personal Information of Residents of the Commonwealth, and its applicability to your business. You wrote the letter as a follow-up to a telephone conversation we had on January 3, 2011, in which you sought information concerning the encryption requirements of 201 CMR 17.00. You have asked that I review an article you published on your website concerning your conclusions as to which tapes are exempt from encryption.

As I explained during our initial telephone conversation, I cannot provide you legal advice concerning which tapes used in your business are covered by the regulations and which are not covered by the regulations due to the fact that such an analysis involves a fact-specific, technological determination that you must make based on your knowledge of the technological capabilities of the tapes and how they are used in connection with your business in terms of portability. I am not authorized to undertake such an analysis to ensure your company's specific compliance with the regulations nor am I authorized to provide a legal opinion attesting to your company's compliance. Specifically, the Office of the Attorney General is limited to providing opinions pursuant to G.L. c. 12, §§ 3, 6, and 9, to officials acting in their official capacity. We are not permitted to offer legal opinions other than in this context, or in the pursuit of litigation on behalf of the Commonwealth.

As I noted during our telephone conversation, I will direct you to 201 CMR 17.04 which states:

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:



(3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(5) Encryption of all personal information stored on laptops or other portable devices;

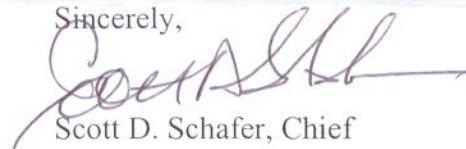
In addition, the Frequently Asked Questions (FAQs), prepared by the Office of Consumer Affairs and Business Regulation, the agency that drafted the regulation, specifically addressed the data tape issue and the definition of to the extent technically feasible as follows:

**Must I encrypt my backup tapes?** You must encrypt backup tapes on a prospective basis. However, if you are going to transport a backup tape from current storage, and it is technically feasible to encrypt (i.e. the tape allows it) then you must do so prior to the transfer. If it is not technically feasible, then you should consider the sensitivity of the information, the amount of personal information and the distance to be traveled and take appropriate steps to secure and safeguard the personal information. For example, if you are transporting a large volume of sensitive personal information, you may want to consider using an armored vehicle with an appropriate number of guards.

**What does "technically feasible" mean?** "Technically feasible" means that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.

I have provided you all the information that I am permitted concerning the requirements of the regulations and their applicability to data tapes in general. To the extent you need further direction on whether your specific business operations and the technologies involved are implicated by the data security regulations, you may wish to consult legal counsel.

Sincerely,



Scott D. Schafer, Chief  
Consumer Protection Division