



REPLY TO  
ATTENTION OF:

[Office]

Name  
Street Address  
Apartment 3  
Anywhere, NY 00000-0000

Dear [Name]:

On [date] personal information pertaining to you maintained by the Department of [Army/Defense], [contractor company name if applicable] [was/may have been] [stolen/lost/compromised/ publicly released]. The information was contained on a [laptop/website/email/document] and contained your [describe all data elements compromised – name, social security number, home address, date of birth, personal email address, home telephone number, etc.].

[Provide a detailed description of what took place, omitting names of personnel involved and details that could affect ongoing investigations.] STYLE EXAMPLE: An Army laptop computer was stolen from the parked car of an Army recruiter in New Orleans, Louisiana after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 members of the public who were potential recruiting prospects.

The [theft/loss/compromise/release] was immediately reported to [name(s) of local, Army, DoD law enforcement agency(s)] who [is/are] now conducting an [joint] inquiry into the matter. [If a theft, indicate whether we believe the data or the equipment was the target of the theft.] [If applicable, indicate whether the data was password protected, encrypted, etc.] [If a website posting, indicate the information was immediately removed upon discovery]. Although we cannot say with certainty, based on these circumstances we believe the probability is [low, moderate, high] that the information will be acquired and used for an unlawful purpose. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission at its Web site at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>. The FTC urges that you immediately place an initial fraud alert on your credit file. The fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card is changed. The site also provides other valuable information that can be taken now or in the future if problems should develop. The Social Security Administration has a toll-free number, 1-800-772-1213, and additional contact information is found on their web site <http://www.ssa.gov/reach.htm>. You may also want to monitor your credit reports by contacting: Transunion <http://www.transunion.com/index.jsp>; Equifax <http://www.equifax.com/>; and Experian <http://www.experian.com/>.

The above listed actions are not an exhaustive list of protective measures you may choose to take. There may be additional organizations or people with whom you may wish to consult, depending on your circumstances.

[If applicable: The Army is providing credit monitoring services to you for a period of [number] months. This service is being provided at no cost to you. Provide details of the credit monitoring conditions, such as what company, for which credit bureaus, points of contact, etc.]

The Army takes this loss very seriously and is reviewing current policies and practices with a view of determining what can or must be changed to preclude a similar occurrence in the future. [Indicate any special steps being taken]. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you. Should you have any questions, please call [POC name, email and phone number].

Sincerely,

[Signature block of Director level or higher official]

## SAMPLE WRITING STYLE: THEFT OF LAPTOP

On April 12, 2007, an Army laptop computer was stolen from the parked car of an Army recruiter in New Orleans, Louisiana after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 members of the public who were potential recruiting prospects. The compromised information included the name, social security number, home address, date of birth, school, personal email address, and home telephone number of recruiting prospects. The theft was immediately reported to the New Orleans Police Department and to the U.S. Army Criminal Investigation Command, who are now conducting inquiries into the theft.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information on the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.