

December 15, 2008

Attorney General Martha Coakley  
Office of the Attorney General  
One Ashburton Place  
Boston, Massachusetts 02108

Dear Attorney General Coakley:

Pursuant to Mass. Gen Laws ch. 93H, §3 (2007), this letter is to inform you that DAP Products Inc. ("DAP") recently experienced a data security breach affecting the personal information of its employees. Specifically, DAP has reason to believe that the personal information of four (4) of its current and former employees who reside in the State of Massachusetts could have potentially been accessed on or before November 7, 2008 without proper authorization. The personal information affected may include names, addresses, and social security numbers. DAP has determined that 17 attempts were made to open fraudulent credit card accounts using the personal information of one (1) current DAP employee located in Maryland and that one such attempt was made involving one (1) former DAP employee from Maryland who is now located in Ohio. Two of those attempts involving the employee currently located in Maryland were successful and resulted in \$3,000 in fraudulent charges on one account, and \$400.00 in fraudulent charges on the other. DAP has no information that any fraudulent attempts were made with regard to any Massachusetts resident.


Once discovered, DAP immediately undertook the following actions:

- Launched a detailed internal investigation; and
- Reported the incident to the Baltimore City Police Department, the State's Attorney for Baltimore, and the Attorney General for the State of Maryland.

DAP's investigation of this incident is ongoing. In addition to continuing its investigation, DAP plans to send a notice to all of its affected Massachusetts employees no later than December 18, 2008, a copy of which is included for your review.

DAP believes this letter is compliant with the notice requirements listed in Mass. Gen Laws ch. 93H, §3 (2007). If, however, you require additional information or documentation, please do not hesitate to contact me by telephone at 410-779-2201 or by e-mail at [rmayor@dap.com](mailto:rmayor@dap.com). Thank you for your time and attention.

Sincerely,

  
Rita A. Mayor  
Vice-President – Human Relations

Enclosure



You'll  
find us  
in all  
the  
right  
places.®

December \_\_, 2008

Dear [EMPLOYEE NAME]:

At DAP, we take very seriously the confidentiality of our employee-related data, and we have policies and procedures in place to safeguard your privacy. However, despite our efforts, problems can occur.

DAP recently became aware that there may have been an unauthorized access to the personal data of some DAP employees. DAP believes that the access might have occurred when a person or persons, without authority, accessed a database that contains the names, addresses, and Social Security numbers of DAP employees and their dependents. The unauthorized access appears to have occurred between January 17, 2008 and November 7, 2008.

Upon learning of this potential unauthorized access, DAP launched an immediate internal investigation. As part of this investigation, DAP has reported the incident to the Baltimore City Police, to the State's Attorney for Baltimore City and to the Attorney General for the State of Maryland.

While DAP is aware of two possible instances of identity theft which may relate to this unauthorized access, we have no indication at this time that any other employees or their dependents have been affected. However, we want to bring this incident to your attention so that you are aware of the actions you can take to minimize any potential risk of identity theft to you or your dependents.

Enclosed is an easy-to-read set of Frequently Asked Questions that we hope will provide you with the steps you can take to address this type of problem. We sincerely apologize to you for this situation and want to assure you that protecting the security and privacy of your information remains our top priority. We are working to strengthen our data protection systems and procedures and will remain vigilant in protecting your personal information. For more information, contact me by telephone at 410-779-2290 or by e-mail at [identity@dap.com](mailto:identity@dap.com). Please also contact me if you believe you have been a victim of identity theft. Once again, please be assured that your security and privacy are our top concern.

Sincerely,

Rita A. Mayor, Vice-President – Human Relations  
DAP Products Inc.

## **Frequently Asked Questions about Unauthorized Access of Personal Information**

### **1. Does this unauthorized access of personal information mean I am a victim of identity theft?**

No. The fact that your personal information, or that of your dependents, may have been accessed does not mean you or your dependents are a victim of identity theft. Identity theft is the unauthorized use of personal information to commit fraud or other crimes.

### **2. How will I know if I am a victim of identity theft?**

The following may indicate that you are a victim of identity theft:

- One of your creditors informs you that it received an application for credit with your name and social security number that you did not submit.
- You receive account statements with your name and address for goods or services you never requested or ordered, for example, statements from major credit card companies (Visa, MasterCard, American Express, Discover), in-store credit card statements (Home Depot, Lowes, Target, etc.), and utility, cell phone and/or telephone statements.
- Your credit card statements and other bills are being delivered in an unusual or improper manner.
- There are unusual or unrecognized purchases on your credit card statement.
- A collection agency contacts you regarding a default on an account you never opened.
- You receive emails, phone calls, or letters asking you for personal information.

### **3. What precautionary steps can I take?**

- ❖ **Go to the FTC Website** – For tips on how to guard against misuse of personal information, visit the Federal Trade Commission website at <http://www.ftc.gov/>.
- ❖ **Obtain your Free Annual Credit Report** – One way to monitor your financial accounts is to review your credit report. By law you are entitled to one free credit report each year. Request a free report from one of the three major credit bureaus – Equifax, Experian, TransUnion – at [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling 1-877-322-8228.
- ❖ **Contact Equifax, TransUnion or Experian for Assistance with Fraud Alerts and Security/Credit Freezes**
  - **What is a Fraud Alert** - A fraud alert tells creditors to take extra precautions before they open any new accounts or change any existing accounts. A fraud alert can be placed by calling the Fraud Alert numbers listed below for any one of the three credit reporting agencies. You only need to contact one of the three credit bureaus; your request will be shared electronically with the other two agencies.

- **What is a Security/Credit Freeze** - A security/credit freeze prevents third parties from accessing your credit report without your consent. A security freeze costs approximately \$5.00 and must be placed with each of the three credit reporting bureaus for it to appear in their records.\* Because a security freeze can hinder your ability to obtain credit, all three bureaus recommend that applicants plan ahead before placing the freeze. Please note that, unlike fraud alerts, the mechanism for requesting a security freeze and the information required differs for each credit reporting agency: For more information on security credit freezes, contact Equifax, TransUnion or Experian using the contact information listed below or refer to the “Additional Information on Security Credit Freezes” section at the end of this FAQ.

- ❖ **Obtain a Police Report** – If DAP files a police report in your jurisdiction, you have a right to obtain it.

#### 4. What should I do about my dependents?

- ❖ You should take the same precautionary steps you are taking for yourself with regard to your dependents.

#### 5. How can I contact Equifax, TransUnion or Experian?

- ❖ The contact information for these three credit bureaus is listed below:

Equifax Credit Information Services, Inc. P.O. Box 740256 Atlanta, GA 30374 <a href="http://www.equifax.com">www.equifax.com</a> Fraud Alert -1.800.525.6285 Credit Report -1.800.685.1111	TransUnion Credit Bureau P.O. Box 6970 Fullerton, CA 82834 <a href="http://www.transunion.com">www.transunion.com</a> Fraud Alert -1.800.680.7289 Credit Report -1.800.680.7289	Experian P.O. Box 9532 Allen, TX 75013 <a href="http://www.experian.com">www.experian.com</a> Fraud Alert -1.888.397.3742 Credit Report -1.888.397.3742
---	--	--

#### 6. I suspect I am a victim of identity theft? What should I do?

If you find suspicious activity on your account statements or credit report or have reason to believe your information is being misused, the Federal Trade Commission recommends the following four steps:

- Call your local law enforcement agency to file a police report. You should obtain a copy of the police report since many creditors want the information it contains to address fraudulent debts.
- Contact the fraud department of at least one, if not all, of the three credit bureaus at the numbers listed above.
- Close any accounts you suspect have been tampered with, but you should feel free to discuss this with the applicable retailer, credit card company, etc. that you do business with.

\* **Massachusetts Residents:** Identity theft victims (and their spouses) who reside in Massachusetts are not required to pay for a security freeze if they provide a police report or similar document evidencing the identity theft (e.g., an identity theft report or DMV report) to the credit reporting agency.

- File a complaint with the Federal Trade Commission (FTC) at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or at 1-877-ID-THEFT (438-4338).

## 7. Are there any other resources for information on identity theft?

Yes, you may want to consult the following agencies for information regarding identity theft:

- Social Security Administration fraud line: 1-800-269-0271.
- Federal Trade Commission: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or at 1-877-ID-THEFT (438-4338).
- National Association of Attorneys General: [www.naag.org](http://www.naag.org).

\* \* \*

### Additional Information on Security/Credit Freezes.

While we suggest you contact the credit reporting agencies directly, here is additional information on security credit freezes.

- **Equifax** – You may submit a written request or call 1-800-685-1111. A written request must include your name, address, date of birth, Social Security Number, proof of current address (such as a current utility bill), and, if required, payment of applicable fees. Personal checks, American Express, Mastercard, VISA, and Discover Cards are acceptable forms of payment. **Cash through the mail will not be accepted.**

If you are required to pay and are paying by credit card, you must include the following information:

- Name of the person as it appears on the credit card
- Type of credit card (American Express, Mastercard, VISA, or Discover Card)
- Complete account number
- Expiration date (month and year).
- Card Identification Number (for American Express: – the 4 digit number on the front of card above the account number; for Mastercard, VISA, or Discover Card: the 3 digit number on back of card at the end of the account number).

If you are an identity theft victim and are requesting a security freeze, you must also include a copy of a police report, identity theft report, or other government law enforcement agency report, such as a DMV report. All written requests must be sent to: **Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348.**

- **TransUnion** – You must submit a written request. Your request must include your name, address, Social Security Number, and a credit card number with expiration date to pay the applicable fee, if any, for the service. You must also include proof of your current residence, such as a state issued identification card or driver's license. All written requests must be sent to: **TransUnion, Fraud Victim Assistance Department, P.O. Box 6790 Fullerton, CA 92834.**
- **Experian** – You must submit a written request. Your request must include your full name, with middle initial and generation (e.g. Jr., Sr., II, III, etc.); Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years; one copy of a government issued identification card (e.g. driver's license, state or military ID card, etc.); one copy of a utility bill, bank or insurance statement, etc.; and a fee of \$5.00 or a valid investigative or incident report or complaint with a law enforcement agency or the DMV. All written requests must be sent to: **Experian Security Freeze, P.O. Box 9554, Allen, TX 75013.**