

# JONES DAY

222 EAST 41ST STREET • NEW YORK, NEW YORK 10017.6702  
TELEPHONE: 212.326.3939 • FACSIMILE: 212.755.7306

JP002158:jjb  
599928-060001

April 29, 2010

**U.S. Certified Mail / Return Receipt Requested**

The Honorable Michael A. Delaney  
Office of the Attorney General  
33 Capitol Street  
Concord, New Hampshire 03301

Re: Recent J.M. Smucker Unauthorized Data Exposure

Dear Honorable Michael A. Delaney:

I am writing to inform you of a recent and unfortunate incident involving an unauthorized data exposure incident affecting our client, The J.M. Smucker Company (“Smucker”), and an estimated 5,976 of its employees and some of their dependents, one (1) of whom resides in your State.

The specific incident involved a transfer of information via Smucker e-mail by a Smucker employee to a relative, who is a computer programmer but not a Smucker employee, for technical assistance with a Human Resource Systems project. This e-mail was sent to a single individual to a secure server at another local company with whom my client has a good working relationship. My client discovered this incident on April 5, 2010 through an internal monitoring tool, and its investigation revealed that certain files containing personal data were attached to this e-mail and that the employee had previously shared Smucker files containing personal information with this same relative. These transfers of information were not done in accordance with the Smucker’s normal procedures for handling employee personal data and have resulted in disciplinary actions.

The following information was included in the files shared with the relative: employee identification number, last name, first name, middle initial, Smucker e-mail address, home address, hire date, birth date, YTD taxable income, YTD supplemental wages, and social security number. In some instances, the following information about employees’ dependents was also included in the shared files: last name, first name, middle initial, home address, birth date, and social security number.

Through communications with the employee and the relative, Smucker does not believe that there was any malicious intent, but that the transmission was made due to a lack of proper judgment. Further, through my client’s extensive investigation and cooperation of the security and legal personnel from the receiving company, my client has determined the personal data was

NYI-4272049v3

Honorable Michael A. Delaney  
April 29, 2010  
Page 2

successfully contained and was not distributed or maintained by the employee or the employee's relative.

In addition to the actions referenced above, the Federal Bureau of Investigation (the "FBI") was also immediately contacted and they completed an independent review to assess any exposure risks. The findings of their investigation supported the results of Smucker's internal investigation and they also concluded that there was no malicious intent.

Smucker obtained possession of the employee's work and home computer and arranged for an independent third party provider to conduct further forensic analysis to verify there was no further exposure of the personal information. My client has also been in contact with the relative's employer, and they subsequently disabled access to the programmer's work computer, quarantined the e-mail, removed it from their system, and confirmed that the e-mail and attachment were neither forwarded nor extracted from their systems. Again, Smucker is confident that the information was contained.

Smucker anticipates that it will begin notifying all affected employees and affected dependents (if any) who have been identified on April 29, 2010. An exemplar copy of the notice letter is enclosed for your information. As the enclosed letter explains, Smucker has taken numerous steps to protect the security of the affected employees, including notifying the FBI, providing affected employees with a full package of credit protection service and credit insurance for one year free of charge, establishing a toll-free number that employees can call for further information and assistance, as well as notifying the major national credit reporting agencies where required by law.

Smucker has taken steps to reduce the risk of future unauthorized data transmissions or exposures and is continuing to carefully monitor this situation. Should any significant new information arise, we will promptly inform you.

Please do not hesitate to contact me if I can provide you with any additional information.

Best regards,

A handwritten signature in blue ink, appearing to read "Mauricio F. Paez", with a long horizontal stroke extending to the right.

Mauricio F. Paez

Enclosure

Honorable Michael A. Delaney  
April 29, 2010  
Page 3

cc: M. Ann Harlan, Esq. (Vice President and General Counsel)  
Shannon L. Shinaberry, Esq. (Director, Human Resources - Operations  
and Assistant General Counsel)



*Since 1897*

April [ ], 2010

<title> <first name> <last name>  
<address>  
<city>, <state> <postal code>

Dear <title> <last name>:

As you know, The J. M. Smucker Company takes very seriously our responsibility to safeguard all sensitive and confidential information regarding employees, customers, consumers, suppliers or other individuals and organizations. For this reason we have strict Company-wide policies, procedures, and system controls to protect our confidential information.

We are writing to inform you of an unfortunate incident pertaining to the violation of Company procedures which involved an employee making an unauthorized transfer of certain files containing a number of Smucker's employees' personal information, including yours, which was sent to a relative of that employee. We identified the transfer through a Company security program and immediately recovered and secured the files containing the personal information.

***Please be assured we thoroughly investigated the matter and have no indication of any unauthorized us of this personal information, nor do we believe there was any intent to use this information.***

Nonetheless, we regret this incident occurred and consistent with our policy of open and transparent communications we wanted to make you aware of the issue. In addition, out of an abundance of caution we want to assure you we are taking special precautionary measures because of this incident to help protect your privacy and security.

#### **Details of Incident and Investigation**

These incidents involved transfers of employee personal data by a Smucker employee via Smucker e-mail to a relative, who is a computer programmer but not a Smucker employee, for technical assistance with Human Resource Systems projects. The e-mail was sent on April 5, 2010 to a single individual to a secure server at another local company with whom we have a good working relationship. Our investigation revealed that certain files containing personal data were included in these unauthorized file transfers and that the employee had previously shared Smucker files containing personal information with this same relative. These transfers of information were not done in accordance with the Company's normal procedures for handling employee personal data and have resulted in disciplinary actions.

The following employee personal information was included in the transmission: employee identification number, last name, first name, middle initial, Smucker e-mail address, home address,

hire date; birth date, year-to-date taxable income, year-to-date supplemental wages, and social security number. In addition to the employee personal data, the following personal information relating to dependents of some Smucker employees was also included in the shared files: last name, first name, middle initial, birth date, and social security number. Unfortunately, we have identified your personal information in the files that were transferred. If your dependent information was also included in the transferred files, a "Your Company-Provided Triple Alert Membership" packet included with this letter identifies each such non-minor (over 18 years-old).

Through our communications with the employee and the relative, we do not believe that there was any malicious intent, but that the transmissions were made due to a lack of proper judgment and to facilitate off-site work by the employee. Further, through our extensive investigation and cooperation of the security and legal personnel from the receiving company, we are confident the personal data was successfully contained, was not distributed and is no longer maintained by the employee or the employee's relative.

In addition to the actions referenced above, the Federal Bureau of Investigation (the "FBI") was also immediately contacted and they completed an independent review to assess any exposure risks. The findings of their investigation supported the results of our internal investigation and they also concluded that there was no malicious intent.

We also obtained possession of the employee's work and home computers and arranged for an independent third party provider to conduct further forensic analysis to verify there was no further exposure of the personal information. The Company has also been in contact with the relative's employer, and they subsequently disabled access to the programmer's work computer, quarantined the e-mail, removed the files from their system, and confirmed that the e-mail and attachment were neither forwarded nor extracted from their systems. Again, we believe the information was contained.

### **Company Assistance to Protect Your Privacy and Security**

Despite our confidence that the information was contained, Smucker is acting with an abundance of caution to help you protect your privacy and security. Attached you will find information on the steps we have taken to help you detect possible misuse of your information as well as tips and contact information that will help you remain vigilant against the possibility of fraud and/or identity theft.

As part of this assistance Smucker is providing affected employees and their affected non-minor (over 18-years old) dependents with a free one-year membership in Triple Alert<sup>SM</sup> from ConsumerInfo.com, Inc. an Experian® company. Triple Alert will provide you with world-class credit monitoring capabilities and in-depth assistance in every aspect of identity theft protection including identity theft insurance. Triple Alert is provided to you completely free of charge by Smucker and enrolling in this program will not impact your credit score. We have attached detailed information on your company-provided Triple Alert membership and instructions on how to activate it. Triple Alert membership instructions are included for your dependents only if their information was affected by this incident.

We deeply regret this incident and any inconvenience or concern this may cause you. We want to assure you that the Company has been diligently addressing this matter to minimize risk from this issue.

Please feel free to contact your local Human Resource Representative if you have additional questions.

Sincerely,



Barry Dunaway  
Senior Vice President  
Corporate and Organization Development



Andy Platt  
Vice President  
Information Services, CIO

## Company Assistance to Protect Your Privacy and Security

Despite our confidence that the personal employee and dependent information involved in this event was contained, we have acted with an abundance of caution to protect the privacy and security of our affected employees and their families. We advise that you remain vigilant against the possibility of fraud and/or identity theft by monitoring your account statements and credit reports for unusual activity. To help you to protect yourself, and your dependents where necessary, Smucker has taken the following steps:

- To help you detect the possible misuse of your information, we are providing you and your non-minor (over 18 years-old) dependents with a free one-year membership in Triple Alert<sup>SM</sup> from ConsumerInfo.com, Inc. an Experian® company to provide you with world-class credit monitoring capabilities and in-depth assistance in every aspect of identity theft protection including identity theft insurance\*. Triple Alert is provided to you completely free of charge by Smucker and enrolling in this program will not impact your credit score. Please see “Your Company-Provided Triple Alert Membership” below for instructions on how to activate your company-provided Triple Alert and details on the membership.
- We have also taken the same steps to protect the privacy and security of your non-minor dependents' personal information, including offering them with the same one-year free membership in Triple Alert, which we are providing to you. An individual activation code for Triple Alert for each such affected non-minor dependent is also provided below.
- Smucker has set up a special toll-free number, **1-888-815-6842**, to provide you with further assistance and information you may need regarding this incident. (Questions specific to the company-provided Triple Alert memberships should be directed to Experian at the number listed below.)
- In some states, the Company has notified the Attorney General's office or other state agencies as required by law.
- In some states, Smucker has also contacted the three major U.S. credit agencies to inform them of these incidents, as required by law. This was a general report and none of your or your dependents personal information was provided.

## Additional Protection

For your additional protection, we suggest you contact the fraud department at any one of the three credit agencies to inform them that you may be a potential victim of identity theft and request that a “fraud alert” be placed on your credit file. A fraud alert is a consumer statement added to your credit file that warns creditors about possible fraudulent activity within your account and requests that any creditors contact you before they open any new accounts or change your existing accounts. There is no charge for this service, and it is easy to request. Call any one of the three major credit agencies listed below. As soon as you alert one credit agency, it will notify the other two to place fraud alerts on your account as well.

<b>Credit Agency</b>	<b>Fraud Alert Toll-Free No.</b>	<b>Website</b>
Equifax	1-888-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

In addition to the steps Smucker has already taken to protect you, there are a number of other ways you can protect yourself from fraud and identity theft:

- You are entitled under U.S. law to one free credit report annually from each of the three major credit agencies listed above. Reviewing your credit report will allow you to confirm that no new accounts have been opened without your knowledge and may give you early notice of any potential fraud or incidents of identity theft. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free [1-877-322-8228](tel:1-877-322-8228).
- When you receive your credit reports, review them carefully. If you see anything you do not understand, call the credit reporting agency. If you do find suspicious activity on your credit reports, call your local police or sheriff’s office and file a police report of identify theft. Make sure to obtain a copy of the police report because you may need to provide the report to creditors to clear your record. You also should file a complaint with the Federal Trade Commission (“FTC”) at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or at 1-877-ID-THEFT (1-877-438-4338). Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.
- Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you continue to check your credit reports periodically. Identity thieves sometimes hold on to personal information for a period of time before using it. Checking your credit reports periodically can help you spot potential problems and address them quickly.
- For additional information on how to further protect yourself against identity theft, you may wish to visit the website of the U.S. Federal Trade Commission at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).



## **Your Company-Provided Triple Alert Membership**

To activate your company-provided one year membership in Triple Alert from Experian, visit the website listed below and enter your individual activation code. If you prefer, you can enroll on the phone by speaking with Experian Customer Care representatives toll-free at [1-866-252-0121](tel:1-866-252-0121).

**Triple Alert Web Site: [site]**  
**Your Activation Code: [Activation Code]**  
**You Must Enroll By: [Expiration date]**

As soon as you enroll in your company-provided Triple Alert membership, Experian will begin to monitor your credit reports from Experian, Equifax<sup>®</sup> and TransUnion<sup>®</sup> on a daily basis and notify you of key changes. This powerful tool will help you identify potentially fraudulent use of your information, and provide you with immediate assistance from a dedicated team of fraud resolution representatives should you ever need help.

### **Your Company-provided 12-month Triple Alert membership includes:**

- Daily monitoring and timely alerts of any key changes to your credit reports—so you know when there is any activity that you should be made aware of such as notification on new inquiries, newly opened accounts, delinquencies, public records or address changes
- Toll-free access to a dedicated team of fraud resolution representatives who will help you investigate each incident; contact credit grantors to dispute charges, close accounts if need be, and compile documents; and contact all relevant government agencies
- \$25,000 in identity theft insurance coverage (\$10,000 for New York state residents) with zero deductible provided by Virginia Surety Company, Inc. for certain identity theft expenses

Once your enrollment in Triple Alert is complete, you should carefully review your credit reports for potentially inaccurate or suspicious items. If you have questions about Triple Alert, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care at [1-866-252-0121](tel:1-866-252-0121).