



Christopher J. Dilenno
D: 215.358.5161
C: 610.283.5286
cdiienzo@nldhlaw.com

518 Township Line Road
Suite 300
Blue Bell, PA 19422
P: 215.358.5100
F: 215.358.5101

January 6, 2014

Attorney General Michael A. Delaney
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: U.S. Fund for UNICEF— Notice of Data Security Event

Dear Sir or Madam:

We represent the U.S. Fund for UNICEF (“U.S. Fund”), 125 Maiden Lane, New York, NY 10038, and are writing to notify you of a data event that compromised the security of personal information of three (3) New Hampshire residents. The U.S. Fund’s investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the U.S. Fund does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On or about December 2, 2013, U.S. Fund discovered that an unauthorized individual or individuals gained access to one of the U.S. Fund’s servers on or about November 4, 2013. Upon discovery, the U.S. Fund immediately disabled the affected server and disconnected it from the U.S. Fund’s network. The U.S. Fund then launched an investigation to confirm the full scope of the incident and to identify all individuals whose information may have been exposed. The U.S. Fund retained specialized data security counsel to assist with its investigation of, and response to, this incident. The U.S. Fund hired independent, third-party computer forensics experts to determine the scope of this incident and to confirm the identities of all individuals whose information may have been exposed. Although the various investigations are ongoing, the U.S. Fund has determined that this attack was limited to one server. The U.S. Fund’s staff reviewed all of the information that may have been exposed and has determined that a portion of this exposed information contained personal information.

Notice to New Hampshire Residents

Although the investigations are ongoing, the forensic experts hired by the U.S. Fund confirmed that this event resulted in the unauthorized access to the name, phone number, credit card information, including the security code and expiration date (if provided), and in some cases bank account information of three (3) New Hampshire residents. Upon confirmation of this attack by our forensic experts, the U.S. Fund provided these New Hampshire residents with written notice of this incident on or about January 6, 2014, in substantially the same form as the letter attached here as Exhibit A.

Other Steps Taken and To Be Taken

The U.S. Fund takes this matter, and the security of the personal information in its care, seriously and has taken measures to ensure that this type of exposure does not occur again. In addition to providing written notice of this incident to affected individuals as described above, each affected individual is being offered access to one (1) free year of credit monitoring services and identity restoration services. The U.S. Fund is providing each individual with information on how to protect against identity theft and fraud. The U.S. Fund notified its merchant bank of this incident. U.S. Fund is providing written notice of this incident to other state regulators where required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-358-5161.

Sincerely,



Christopher J. Dilenno

cc: U.S. Fund for UNICEF

Exhibit A

[Date]

[Name]

[Address]

[City, State Zip]

Dear [Name]:

We are writing to notify you of an incident that may affect the security of your personal information.

On December 2, 2013, the United States Fund for UNICEF ("U.S. Fund") discovered that an unauthorized individual or individuals gained access to one of the U.S. Fund's servers on or about November 4, 2013. Upon discovery, the U.S. Fund immediately disabled the affected server and disconnected it from our network. We then launched an investigation to confirm the full scope of the incident and to identify all individuals whose information may have been exposed. While our investigation into this incident is ongoing, the initial results have determined that the unauthorized access was limited to one server. We have taken measures to ensure this type of exposure does not occur again.

The U.S. Fund takes this matter, and the security of your personal information, extremely seriously. In addition to its own internal investigation, the U.S. Fund has retained third party forensic experts and data privacy security legal counsel to assist with its investigation. Upon review, it has been determined that a portion of the exposed information may have contained personal information. Although these investigations are ongoing, there is a possibility that the unauthorized access of the U.S. Fund's server may have resulted in access to your personal information, including your name, credit card number, credit card security code and expiration date (if provided to us), bank account number, your phone number, and your email address.

Although we have no evidence to date of attempted or actual misuse of your information, as a precaution, we retained AllClearID to provide identity protection services for one year at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next year.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use this service – there is no action required on your part. If a problem arises, simply call «DID_Phone» and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling «DID_Phone» using the following redemption code: {RedemptionCode}.

Please note: Additional steps may be required by you in order to activate your phone alerts for the PRO service.

While we stand ready to assist you fully, you may also take action directly to further protect against possible identity theft or other financial loss. We encourage you, to review your account statements regularly, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file.

Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below. Information regarding security freezes is also available from these agencies.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

You can further educate yourself regarding identity theft, security freezes, and the steps you can take to protect yourself, by contacting the Federal Trade Commission. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-ID-THEFT (877-438-4338); TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

Though we are vigilant in protecting the privacy of our donors, there are clearly unscrupulous entities seeking to access our information systems. We are saddened at this occurrence, and I apologize for any inconvenience or concern that this may have caused. We hope we can enjoy your support in the future. To further assist you, we have established a confidential privacy line, staffed with professionals trained in credit and identity protection and familiar with this incident. If you have any questions regarding the incident or the information in this letter, please contact this confidential privacy line at X-(XXX) XXX-XXXX. This line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. E.S.T.

Very truly yours,

Edward G. Lloyd
Chief Operating Officer and Chief Financial Officer
United States Fund for UNICEF