National Capital Poison Center

NEWS RELEASE

Media Contact:
Toby Litovitz, MD
(202) 362-7493
pc@poison.org

National Capital Poison Center Provides Notice of Potential Data Security Incident

Washington, D.C., December 8, 2017 – Although it has no indication or reports of unauthorized access or acquisition of data, National Capital Poison Center ("NCPC") in Washington, D.C., announced today that it has taken action after becoming aware of an incident in which an unknown third party may have gained access to information collected during calls to or from the NCPC call center. Out of an abundance of caution, NCPC is providing notice of the event to potentially impacted individuals, as well as certain regulators and consumer reporting agencies.

Importantly, this information does not include Social Security numbers, driver's license numbers, passport numbers, government identification numbers, financial account information, credit card information, or debit card information.

Additionally, this incident was isolated to the NCPC located in Washington, D.C., and did not affect the other 54 U.S. poison centers. NCPC predominantly serves the Washington D.C. metro area, but receives some calls from every state. Online poison control services provided through webPOISONCONTROL® and NCPC's donor database were <u>not</u> affected.

"NCPC takes the security of information stored on our systems very seriously, and we understand this incident may cause concern or inconvenience," Dr. Toby Litovitz, Executive and Medical Director of NCPC, said. "We continue to work with third-party forensic investigators to ensure the security of our systems, and encourage people to contact us at 877-218-3009 (U.S. and Canada callers) or 814-201-3664 (international callers) with any questions or concerns."

What Happened? In October 2017, NCPC discovered it had experienced a ransomware infection. Upon discovery of this incident, NCPC immediately launched an investigation, with the assistance of a third-party forensic investigator, to determine the nature and scope of the event and ensure the security of their systems. While this investigation is ongoing, on November 27, 2017, NCPC determined that unauthorized access to a database server occurred on October 21, 2017, and that unauthorized access to the data stored on that server cannot be ruled out. The possibly affected database contains information provided during calls made to or from the center between January 1997 and October 21, 2017.

What Information Was Involved? NCPC cannot determine whether any information stored in the database was subject to unauthorized access, and has received no reports of attempted or actual misuse of this information. The database server contains one or more of the following types of information captured during call center calls, if the information was provided: caller name, name of person possibly exposed to a poisonous substance and date of birth, address and telephone number, information about the exposure and clinical course, recommendations provided to the caller, caller's email address, and if applicable, treating facility name and medical record number. Most calls have only a subset of this information.

What We Are Doing. NCPC immediately launched an investigation into the incident, with the assistance of a third-party forensic investigation firm. While this investigation is ongoing, NCPC additionally ensured the security of its information systems and is actively monitoring its information systems for suspicious activity. Since NCPC has insufficient contact information for the majority of individuals whose information may be contained in the caller records, NCPC will provide substitute notice to potentially impacted individuals by way of a notice on the homepage of the NCPC website, www.poison.org, as well as publishing notice to certain state media outlets and in certain state media publications. NCPC will mail notice letters to those individuals for whom NCPC has confirmed mailing address information and who reside in states affording protection to the type of information contained in the database.

For More Information. NCPC has established a dedicated assistance line for individuals seeking additional information regarding this incident. While we have no evidence that any information was misused, if you believe you were impacted by this incident, you can call 877-218-3009, 9 a.m. to 7 p.m. ET, Monday through Friday, excluding major holidays, and Saturdays and Sundays from 11 a.m. to 8 p.m. ET. Individuals calling from outside the United States and Canada may call 814-201-3664 (phone provider fees may apply).

What You Can Do. While the types of information that are potentially compromised as a result of this incident are not those that can be easily used to perpetrate identity theft, fraud, harm, or loss, and NCPC has received no reports of actual or attempted misuse of the information involved in this incident, NCPC encourages everyone to remain vigilant against incidents of identity theft by reviewing their account statements regularly and monitoring their credit reports for suspicious activity. Under U.S. law, individuals over the age of 18 are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report.

NCPC encourages individuals who believe they may be affected by this incident to take additional action to further protect against possible identity theft or other financial loss. At no charge, individuals can also have these credit bureaus place a "fraud alert" on their credit file that alerts creditors to take additional steps to verify their identity prior to granting credit in their name. Note, however, that because it tells creditors to follow certain procedures to protect the individual, it may also delay their ability to obtain credit while the agency verifies their identity. As soon as one credit bureau confirms the individual's fraud alert, the others are notified to place fraud alerts on the individual's file. Should the individual wish to place a fraud alert, or should the individual have any questions regarding his or her credit report, the individual can contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

An individual may also place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from an individual's credit report without

the consumer's written authorization. However, individuals should be aware that placing a security freeze on their credit report may delay, interfere with, or prevent the timely approval of any requests they make for new loans, credit mortgages, employment, housing, or other services.

If an individual has been a victim of identity theft, and the individual provides the credit reporting agency with a valid police report, it cannot charge the individual to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge a fee of up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. Individuals will need to place a security freeze separately with each of the three major credit bureaus listed above if the individual wishes to place the freeze on all of their credit files. In order to request a security freeze, you will need to supply the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit file report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

To find out more on how to place a security freeze, individuals can contact the credit reporting agencies using the information below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 (NY residents please call 1-800-349-9960) www.freeze.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion PO Box 2000 Chester, PA 19022-2000 1-888-909-8872 www.transunion.com/securityfreeze

Individuals can further educate themselves regarding identity theft, fraud alerts, and the steps they can take to protect themselves, by contacting the Federal Trade Commission or their state Attorney General. *For Rhode Island Residents:* The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401)247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. The total number of impacted Rhode Island residents is not known.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft/, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Individuals 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. This notice has not been delayed by law enforcement, and the total number of impacted individuals is not known.

About the National Capital Poison Center

The National Capital Poison Center, founded in 1980, is an independent, private, not-for-profit 501(c)(3) organization and accredited poison center. Its nurse and pharmacist Certified Specialists in Poison Information and medical toxicologists provide 24/7 telephone guidance for poison emergencies, free of charge. Service focuses on the metro D.C. area with a national scope for projects such as web**POISON**CONTROL®, the National Battery Ingestion Hotline, and The Poison Post®. The mission of the National Capital Poison Center is to prevent poisonings, save lives, and limit injury from poisoning. In addition to saving lives, Poison Control decreases health care costs of poisoning cases.