



BOYS & GIRLS CLUBS

March 26, 2018

The Honorable Gordon MacDonald
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED

APR 02 2018

CONSUMER PROTECTION

Boys & Girls Clubs
701 N. Raleigh Boulevard
Raleigh, N.C. 27610
(919) 834-6282
(919) 821-2625 (Fax)
www.wakebgc.org

Re: Data Incident Notification

Dear Mr. Attorney General:

To the extent required by New Hampshire Statutes Section 359-C:20, we are writing to notify you about a potential incident affecting information maintained by the Boys & Girls Club of Wake County (the "Boys & Girls Club") related to approximately two New Hampshire residents.

In January 2018, we became aware that an unauthorized third party had gained access to certain servers on our network and installed malware on two of those servers. The servers contained employee information needed to conduct our operations, including paying our employees. We instructed our IT vendor to isolate the malware, launched a thorough investigation, and engaged an independent cybersecurity forensic investigator to analyze the incident to determine what occurred, the nature of the malware and its functionality, and the information that was potentially compromised, review our systems and assist us in securing the affected part of our network. Following discovery of the malware, the affected servers were taken offline and analyzed, and the malware was quarantined, analyzed and removed from the servers.

Based on the forensic investigation, we believe the third party could have accessed certain personal identifying information contained in files stored on our network. Information potentially accessed may include: an employee's first and last name, email address, mailing address, birth date, phone number, Social Security Number and in some cases, bank account information used for direct deposit of employee payments. Based on the current status of the review, we currently have not found evidence that this personal information has actually been accessed or misused.

The Boys & Girls Club takes its obligation to protect the privacy and security of personal information very seriously. After we learned of this matter, we immediately began a detailed investigation into the incident. We took several steps to investigate and limit the exposure of this information:

- We immediately isolated and took offline all affected servers.
- We engaged an independent cybersecurity forensic investigator to analyze the incident to determine what occurred, the nature of the malware and its functionality, and the information that was potentially compromised.
- We engaged outside advisors to help identify and notify potentially affected individuals once it was determined that individual personal information could have been affected.
- We established a call center to answer frequently asked questions, locate current addresses for individuals, and forward the contact information for people who request additional information to our incident response team.

**Raleigh Boys Club • Wake Forest Boys & Girls Club • Raleigh Girls Club
Washington Boys & Girls Club • Zebulon Boys & Girls Club
6584560_3.Docx Brentwood Boys & Girls Club • The Club Teen Center • Camp BTI**

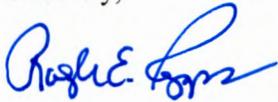
- We are providing two years of free credit monitoring and identity theft protection services to affected individuals whose personal information was contained in the potentially compromised files. Enrollment instructions are included in the notification letters sent to affected individuals.

We are committed to making improvements in our security procedures and practices to help prevent this type of incident from happening again. We have taken numerous steps to review and enhance our cybersecurity practices, and we will continue to work closely with our internal team and outside IT security consultants to implement long-term security improvements and practices.

New Hampshire residents who potentially may be affected are being provided written notification pursuant to N.H. Rev. Stat. § 359-C:20 via U.S. mail on or about the date first written above. A sample copy of the notification letter is enclosed.

Please direct any questions or comments to me at rcapps@wakebgc.org or (919) 834-6282.

Sincerely,



Ralph E. Capps
President/CEO
Boys & Girls Clubs
701 N. Raleigh Blvd,
Raleigh, NC 27610
(919) 834-6282
rcapps@wakebgc.org

Enclosure



BOYS & GIRLS CLUBS

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 23, 2018

Re: Data Incident Notification

Dear John Sample,

As either a current or former worker in our Boys & Girls Clubs, we very much value your commitment to our organization. We also respect the privacy and security of your information, which is why, as a precautionary measure, we are writing to let you know about an event that may involve some of your personal information.

What Happened and What Information Was Involved?

In connection with a recent investigation, the Boys & Girls Clubs became aware that an unauthorized third party gained access to certain servers on our network and installed malware on certain servers. Based on this investigation, we believe this incident may have involved some or all of the following information: your first and last name; your Social Security number; your driver's license number; and certain financial account information. Based on what we currently know, the investigation did not reveal evidence that this personal information has actually been accessed or misused.

What We Are Doing

We take our obligation to protect the privacy and security of personal information very seriously. We learned of this matter in January 2018, and immediately engaged a cybersecurity team to investigate further. Upon learning of the incident, we isolated the affected servers, and the malware was quarantined and removed from the servers. Shortly after this, the forensic team began its analysis. We have identified several areas that needed attention, and implemented solutions to improve our overall capabilities in those areas. We are taking additional precautionary measures that include implementing enhanced capabilities for monitoring suspicious activity. We have also notified the Attorney General's Office about this incident. In addition, we intend to provide additional training to employees on detecting and preventing this type of security incident. We are also evaluating additional safeguards that will expand our abilities to prevent similar occurrences from happening in the future.

Credit Monitoring and Identity Protection

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months 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 24 months.



01-02-1-00

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-288-3423 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in this 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 1-855-288-3423 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Steps You Can Take to Protect Your Information against Misuse

- You should remain vigilant against the possibility of fraud or identity theft by monitoring your credit reports for unusual activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.
- If you ever suspect that you are a victim of identity theft, you should report the incident to local law enforcement or the Attorney General's Office.
- Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports and financial reports periodically. Once a year you may obtain a free copy of your credit report from each of the three credit reporting agencies, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report at www.annualcreditreport.com, by calling 1-877-322-8228, or by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA, 19022
1-800-888-4213
www.transunion.com

- When you receive credit reports, review them carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not contact. Look for personal information such as home address or Social Security number that is not accurate. If you see anything you do not understand, call the consumer reporting agency at the telephone number listed on the report. If you find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft.
- You have the right to request a police report of identity theft. You may need to give copies of the police report to creditors to clear up your records.

- You have the right to place a fraud alert on your credit files. There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. Call or write one of the three consumer reporting agencies as specified below to place a fraud alert on your credit files.

Equifax
 P.O. Box 740241
 Atlanta, GA 30374-0241
 1-866-349-5191
 www.equifax.com

Experian
 P.O. Box 9532
 Allen, TX 75013
 1-888-397-3742
 www.experian.com

TransUnion
 P.O. Box 2000
 Chester, PA 19016
 1-888-909-8872
 fraud.transunion.com

- You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit. If you place a security freeze on your credit report, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state and by credit reporting agency, generally \$5 to \$20 per action at each credit reporting company. However, this fee may be waived under certain circumstances if, for example, you are the victim of identity theft or the spouse of a victim of identity theft. Unlike a fraud alert, if you wish to place a security freeze on your credit report with multiple consumer reporting agencies, you must directly contact each consumer reporting agency. For more information on how to obtain a security freeze, please contact the FTC or one of the three major consumer reporting agencies as specified below.

Equifax
 P.O. Box 740241
 Atlanta, GA 30374-0241
 1-800-685-1111
 www.equifax.com

Experian
 P.O. Box 9532
 Allen, TX 75013
 1-888-397-3742
 www.experian.com

TransUnion
 P.O. Box 2000
 Chester, PA 19016
 1-888-909-8872
 freeze.transunion.com

- Because your Social Security number, address and wage information were involved, the IRS recommends that you file your taxes early before scammers try to obtain a fraudulent tax refund using your Social Security number. If you suspect or know you are the victim of tax-related identity theft, you should complete and submit IRS Form 14039 (Identity Theft Affidavit) to the IRS. IRS Form 14039 is available at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>. If you file IRS Form 14039, the IRS will flag your account to identify questionable activity, and may require additional steps to file your tax return.

To obtain more information about preventing identity theft, contact the Federal Trade Commission: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-438-4338, www.ftc.gov/idtheft.



The Boys & Girls Clubs remain committed to ensuring the privacy and security of personal information. If you have further questions or concerns about this incident, contact me at 919-834-6282 or rcapps@wakebgc.org.

Sincerely,

A handwritten signature in cursive script that reads "Ralph".

Ralph E. Capps, President & CEO
Boys & Girls Clubs
701 N. Raleigh Boulevard
Raleigh, NC 27610