

RECEIVED

AUG 30 2019

BakerHostetler

CONSUMER PROTECTION
Baker & Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Eric A. Packel
direct dial: 215.564.3031
epackel@bakerlaw.com

August 29, 2019

VIA OVERNIGHT MAIL

Gordon MacDonald
Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Fedcap Rehabilitation Services, Inc. ("Fedcap"), to notify you of a security incident. Fedcap is a nonprofit organization that provides vocational training and employment resources to those who face barriers to employment, and maintains information related to those services.

On May 28, 2019, Fedcap concluded its investigation and analysis of an incident related to wire transfer fraud via access to employee email accounts. Upon learning of the suspected wire fraud, Fedcap launched an investigation with the assistance of a leading cybersecurity firm. The investigation determined that an unauthorized party had accessed seven Fedcap employee email accounts between September 20, 2018 and January 27, 2019. As part of its investigation, Fedcap undertook a comprehensive review of the email accounts and determined that they may have contained information pertaining to current and former clients and employees. The information varied by individual, but may have included names in combination with dates of birth, Social Security numbers, driver's license numbers, passport numbers, financial account numbers with PINs / security codes, and payment card information. To date, there is no evidence that any of the personal information in the email accounts was misused as a result of the incident.

Beginning on August 29, 2019, Fedcap will mail notification letters via United States Postal Service First-Class mail to seventy-two (72) residents in accordance with N.H. Rev. Stat. § 359-C:20, and where applicable, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and its Regulations including 45 C.F.R. § 164.404.¹ A copy of the notification letter is enclosed. Individuals whose Social Security or driver's license numbers were involved are being offered complimentary one-year memberships in credit monitoring services through Experian®.

¹ Notice is also being provided to an additional seventy-eight (78) New Hampshire residents, pursuant to the HIPAA (45 C.F.R. § 164.404).

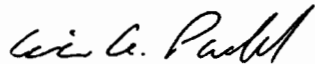
Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

New Hampshire Office of the Attorney General
August 29, 2019
Page 2

Fedcap has taken steps to help prevent a similar incident from occurring in the future, including the implementation of multi-factor authentication, as well as additional procedures to further expand and strengthen its security processes.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Eric A. Packel". The signature is written in a cursive style with a large initial "E".

Eric A. Packel

Enclosure

Fedcap Rehabilitation Services, Inc.
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



August 29, 2019

[REDACTED]

Dear [REDACTED],

Fedcap Rehabilitation Services, Inc. ("Fedcap") takes data security very seriously, and we understand the importance of protecting the information we maintain. We are writing to inform you about an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On May 28, 2019, Fedcap concluded our investigation and analysis of an incident related to wire transfer fraud via access to employee email accounts. Upon learning of the suspected wire fraud, Fedcap launched an investigation with the assistance of a leading cybersecurity firm. The investigation determined that an unauthorized party had accessed seven Fedcap employee email accounts between September 20, 2018 and January 27, 2019. As part of our investigation, we undertook a comprehensive review of the emails and attachments in the employees' email accounts and determined that they may have contained some of your information, including your name and Social Security number.

Although, to date, we have no evidence that any of your information has been misused, out of an abundance of caution, we wanted to let you know this happened and assure you we take it very seriously. We encourage you to remain vigilant by reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately. If your medical or health insurance information was potentially involved in this incident, we recommend that you regularly review the explanation of benefits received from your health insurer. If you see services that you did not receive, please contact the insurer immediately. As a precaution, we have secured the services of Experian® to offer you a complimentary one-year membership of Experian's IdentityWorksSM. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect yourself, please see the pages that follow this letter.**

We regret any inconvenience or concern this may cause you. We have taken steps to help prevent a similar incident from occurring in the future, including the implementation of multi-factor authentication, as well as additional procedures to further expand and strengthen our security processes. If you have any questions, please call 1-844-535-5016, Monday through Friday, 8am to 5pm, Eastern Time.

Sincerely,

Christine McMahon
Christine McMahon
Chief Executive Officer

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **11/21/2019** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code:** [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **DB14394** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, 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 team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

Regardless of whether you choose to take advantage of the complimentary credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

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

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-IDTHEFT (438-4338)

If you are a resident of Maryland or North Carolina, you may contact and obtain information from your state attorney general at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202,
1-888-743-0023(toll-free within Maryland) / 1-410-576-6300, www.oag.state.md.us

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699,
1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

Fraud Alerts: There are two types of fraud alerts 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company.

For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

In order to request a security freeze, you will need to provide 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 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 the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five 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, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies 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 identity 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.