



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 12, 2021

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent National Board for Certified Counselors, Inc. (“NBCC”) located at 3 Terrace Way, Greensboro, NC 27403 and are writing to notify your office of an incident that may affect the security of some personal information relating to 9,898 known Washington residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, NBCC does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 7, 2020, NBCC became aware of unusual activity on its network. NBCC conducted an immediate investigation and determined that the network was impacted by malware which prevented access to certain files on the system. In response, NBCC began working with third-party forensic investigators to investigate the nature and scope of the event and to determine what information may have been impacted by this event and to whom the information relates. NBCC also notified the Federal Bureau of Investigation (“FBI”) and is assisting, as needed, in the FBI’s investigation.

The investigation determined that the malware was introduced into the system by an unauthorized actor who also accessed and acquired certain files within NBCC’s system. The unauthorized access occurred between August 31, 2020 and September 7, 2020.

NBCC, with the assistance of the forensic specialists, began a thorough, lengthy, and labor-intensive process to identify sensitive information that may have been contained within impacted files, and to identify the individuals whose information may have been impacted. This review concluded on December 28, 2020. NBCC then took steps to notify potentially impacted individuals.

The information impacted includes name, address, Social Security number, date of birth, and credential information.

Notice to Washington Residents

On January 12, 2021, NBCC began providing written notice of this incident to potentially affected individuals, which includes 9,898 known Washington residents. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*. NBCC also posted notice of this event on its website, as well as issued a press release nationwide. NBCC's review of impacted data is ongoing and this notification may be supplemented if it is determined that a significant number of additional Washington residents are impacted.

Other Steps Taken and To Be Taken

Upon discovering the event, NBCC moved quickly to investigate and respond to the incident, assess the security of NBCC systems, and notify potentially affected individuals. NBCC is also working to implement additional safeguards and training to its employees. NBCC is providing complimentary access to credit monitoring services for twelve (12) months through TransUnion to individuals whose personal information was potentially affected by this incident.

Additionally, NBCC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. NBCC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Office of the Attorney General

January 12, 2021

Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Jeffrey J. Boogay".

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/MLL/mep

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<Variable Heading>>

Dear <<Name 1>>:

National Board of Certified Counselors, Inc. (“NBCC”), is writing to advise you of a recent event that may impact the security of certain personal information related to you. We write to provide you with information about the event, steps taken since discovering the event, and what you can do to better protect against potential misuse of your information, should you feel it is appropriate to do so.

What Happened? On September 7, 2020, NBCC became aware of unusual activity on its network. NBCC conducted an immediate investigation and determined that the network was impacted by malware which prevented access to certain files on the system. In response, NBCC began working with third-party forensic investigators to investigate the nature and scope of the event and to determine what information may have been impacted by this event and to whom the information relates. NBCC also notified the Federal Bureau of Investigation (“FBI”) and is assisting, as needed, in the FBI’s investigation.

The investigation determined that the malware was introduced into the system by an unauthorized actor who also accessed and acquired certain files within NBCC’s system. The unauthorized access occurred between August 31, 2020 to September 7, 2020.

NBCC, with the assistance of the forensic specialists, began a thorough, lengthy, and labor-intensive process to identify sensitive information that may have been contained within impacted files, and to identify the individuals whose information may have been impacted. This review concluded on December 28, 2020. NBCC is notifying you because the investigation determined that certain information relating to you may have been included in the impacted files.

What Information Was Involved? The following information about you was potentially exposed: your name, address, Social Security number, date of birth, and credential information. There is no indication that your information was subject to actual or attempted misuse.

What We Are Doing. NBCC is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures, and are working to implement additional safeguards to further secure our information systems. NBCC is also notifying regulatory authorities, as required by law.

As an added precaution, we are also offering twelve (12) months of complimentary access to credit monitoring and identity theft restoration services through TransUnion. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Your Personal Information*. You can also enroll to receive the complimentary services being offered to you.

For More Information. We understand that you may have questions or concerns that are not addressed in this letter. Please call the dedicated assistance line that we have established regarding this incident by dialing 800-578-4417 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding U.S. holidays.

NBCC sincerely regrets any inconvenience or concern this incident may have caused you.

Sincerely,

National Board of Certified Counselors, Inc.

Steps You Can Take to Help Protect Your Personal Information

Enroll in Complimentary Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.
- You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Additional details regarding your monitoring

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, 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 reporting 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.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

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 (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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

[www.transunion.com/
fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300. **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. **New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>. **North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 1,398 Rhode Island residents impacted

by this incident. **Washington D.C. Residents:** the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.