James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

June 20, 2019

INTENDED FOR ADDRESSEE(S) ONLY

VIA E-MAIL

Office of Consumer Protection
Leiopapa A Kamehameha Building
235 South Beretania Street, Room 801
Honolulu, Hawaii 96813
Email: ocp@dcca.hawaii.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent the Oklahoma Department of Securities, 204 North Robinson Avenue, Suite 400, Oklahoma City, Oklahoma, 73102-7001, and write to provide notice to your office of an incident that may affect the security of personal information relating to certain Hawaii residents. This notice may be supplemented if significant facts are learned subsequent to its submission. By providing this notice, the Oklahoma Department of Securities does not waive any rights or defenses regarding the applicability of Hawaii law, the Hawaii data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about December 11, 2018, the Oklahoma Department of Securities (the "Department") received a notice of a vulnerability in its firewall that made a server accessible. The Department took immediate steps to close the vulnerability in their system and took the server offline. The Department launched an investigation into the incident, and hired third party investigators to confirm what information, if any, may have been accessible. Through this investigation, on or about February 14, 2019, the Department determined that the server was accessible, and that the information contained on the server was potentially impacted. The Department reported this incident to the FBI on January 16, 2019 and has cooperated with the FBI's investigation.

On or about April 15, 2019, as the result of a thorough review of the potentially impacted contents of the server, the investigation confirmed a population of potentially impacted individuals. On May 24, 2019, the investigation identified additional individuals who may have been impacted by this incident. The types of personal information potentially impacted in relation to this incident include the following: name, Social Security number, date of birth, driver's license or state identification number, medical or health information and financial account information.

Notice to Hawaii Residents

On May 10, 2019, the Department began mailing written notice of this incident to the affected individuals. On June 20, 2019, the Department notified a second population of individuals identified as potentially impacted. The notified population included one thousand, twenty eight (1,028) Hawaii residents. Written notice will be provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and to Be Taken

After discovering this incident, The Department began an investigation to determine the nature and scope of this incident, including identifying the individuals who may be affected, putting in place resources to assist them, and providing them with notice of this incident. The Department identified and mitigated the issue by closing the vulnerability on the server, taking the server offline, and bringing in third party forensics to assess the incident. The Department has introduced additional steps to strengthen the security of its systems.

The Department is providing potentially affected individuals access to twelve (12) months of credit monitoring and identity restoration services, through Experian. Additionally, the Department is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, 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 identity theft and fraud 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. The Department notified law enforcement of this incident, and is also notifying other state regulators, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:hpf
Enclosure

EXHIBIT A

STATE OF OKLAHOMA
DEPARTMENT OF SECURITIES
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 20, 2019

E7100-L01-0123456 0001 00000001 **********OEL
SAMPLE A SAMPLE - L01 - Individual Notice
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Breach

Dear Sample A Sample:

The Oklahoma Department of Securities ("Department") discovered an incident that may affect the security of your personal information. We write to provide you with information about the incident, steps we are taking in response, and steps you can take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On or about December 11, 2018, the Department received a report of a vulnerability in a firewall that made a Department server accessible. The Department took immediate steps to close the vulnerability in its computer system and took the server offline. The Department launched an investigation into the incident, and hired third party investigators to confirm what information, if any, may have been accessible. The Department reported this incident to the FBI, and has cooperated with the investigation.

What Information Was Involved? On or about April 15, 2019, after a thorough review process, the Department confirmed that your information was contained within the compromised server. Accordingly, the Department determined the following information related to you may have been viewed without authorization: Exposed Data Element 1, Exposed Data Element 2, Exposed Data Element 3.

What Are We Doing? We take this incident and the security of your personal information seriously. The Department identified and mitigated the issue by closing the vulnerability, taking the server offline, and bringing in third party investigators. We are also taking additional actions to strengthen the security of our systems.

We are providing you with information you can use to better protect against identity theft and fraud, as well as access to XX months of complimentary credit monitoring and identity restoration services with Experian. Instructions for enrolling in the credit monitoring services, as well additional information on how to better protect against identity theft or fraud, are included in the attached *Privacy Safeguards*.

What Can You Do? You can review the *Privacy Safeguards* for additional information on how to better protect yourself against identity theft and fraud. You can also enroll to receive the complimentary credit monitoring and identity restoration services described above.

0123456

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 866.506.7888. This toll-free line is available Monday - Friday from 9:00 am to 9:00 pm EST and Saturday/Sunday from 11:00 am to 8:00 pm EST, excluding major national holidays. We apologize for any inconvenience or concern this incident causes you.

Sincerely,
The Oklahoma Department of Securities

Enclosure

E7100-L01

PRIVACY SAFEGUARDS

Enroll in Credit Monitoring.

To help protect your identity, we are offering a complimentary XX months membership to Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** August 30, 2019 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code: ABCDEFGHI**

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 866.506.7888 by August 30, 2019. Be prepared to provide engagement number **ENG #** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR XX -MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 866.506.7888. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* 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.

Monitor Your Accounts.

We also 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

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 (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	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

0123456

For More 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 promptly reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; (888) 743-0023; and www.oag.state.md.us.

For North Carolina residents, North Carolina residents may wish to review information provided by the North Carolina Attorney General, Consumer Protection Division at www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Services Center, Raleigh, NC 27699.

For 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. We encourage you to 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.