GORDON THOMAS HONEYWELL LLP

Direct: (253) 620-6545
E-mail: sfawcett@gth-law.com

January 24, 2020

Via Email (SecurityBreach@atg.wa.gov)

Attorney General's Office
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

RE: Data Incident Notification

To Whom It May Concern:

On behalf of our client, Oostra Rouw & Associates, Inc. (ORA, Inc.), we are writing to notify you of a data breach of the security of personal information involving up to 2,376 Washington residents.

On December 26, 2019, ORA, Inc. experienced a ransomware attack. Upon learning of the incident, ORA, Inc. promptly undertook steps to protect its clients' personal information and commenced a forensic investigation. ORA, Inc. retained a digital forensic firm and legal counsel to determine what information may have been involved and what additional steps could be taken to protect client information. In addition to continuing to monitor this situation, ORA, Inc. is reexamining its current data privacy and security policies and procedures to find ways of reducing the risk of future data incidents.

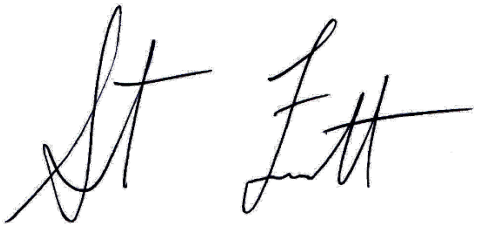
ORA, Inc. also reported the matter to local law enforcement, the FBI and the IRS. ORA, Inc. has been and will continue to work with the IRS to ensure that all necessary steps are taken to prevent and protect from potential fraudulent returns.

ORA, Inc. is notifying all clients whose information may have been compromised and is providing them with information about steps they can take to protect their personal information. On or about January 24, 2019, ORA, Inc. began providing this written notification to all potentially affected persons. The written notification is being provided in substantially the same form as the letter attached hereto as Exhibit A.

ORA, Inc. is committed to protecting the sensitive and protected information of its clients. Should ORA, Inc. become aware of any significant developments concerning this situation, we will inform you as soon as possible.

Should you have any questions regarding this notification or other aspects of this ransomware attack, please contact me at (425) 945-6238 or sfawcett@gth-law.com.

Very truly yours,



Steven Fawcett

Enclosed:
Consumer Notification Letter – Exhibit A

EXHIBIT A

Oostra Rouw & Associates
PO Box 2404 · Mount Vernon, WA 98273

January 24, 2020

«AddressBlock»

Notice of Data Breach

Dear Client,

We are writing to notify you of a recent incident at Oostra Rouw & Associates, Inc. (ORA, Inc.). Although there is no evidence of any data being stolen, we are notifying you because of the sensitive nature of the data you entrust to us. We appreciate the level of trust you place in us — protecting your privacy and security are among our highest priorities.

What Happened: On December 26, 2019, ORA, Inc. experienced a cyberattack called a "ransomware attack." Ransomware is a form of malware that encrypts all the data it can find and holds the computer or network hostage until a ransom is paid.

What Information Was Involved: ORA, Inc. cannot confirm specifically what information, if any, was potentially compromised. However, ORA, Inc. is a tax preparation and bookkeeping firm, therefore, full names, social security numbers, and addresses were present on the computers affected. We are notifying you of this out of an abundance of caution because your information was present and potentially accessible at the time of the ransomware attack.

What We Are Doing: Information privacy and security are among our highest priorities. We have strict security measures in place to protect information in our care. In addition to continuing to monitor this situation, we are taking steps to confirm and further strengthen the security of our systems moving forward.

After immediately identifying and eliminating the threat, our IT company performed a thorough investigation into the incident. Once their internal investigation was complete, we engaged a third-party security expert to conduct an independent assessment of the incident. The unanimous conclusion was that this was a singular event targeting ransom and not data theft.

As a precautionary measure, ORA, Inc. is also providing all relevant regulatory notices and has notified law enforcement and the IRS of the incident.

What You Can Do: We encourage you to remain vigilant against any incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. We recommend that you carefully review the information contained in the enclosed "**Tips to Protect Against Identity Theft and Fraud**" and take any and all steps you deem necessary.

We apologize for any inconvenience or concern this incident may cause you. Please be assured that the privacy of your personal information is important to us. If you have any questions or concerns, please contact us at (360) 336-1040 from 8:00AM to 5:00PM, Monday through Friday.

Sincerely,

Randy Oostra, CPA
Oostra Rouw & Associates, Inc.

Tips to Protect Against Identity Theft and Fraud

Credit Report

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:

- Equifax 1-800-685-1111 www.equifax.com
- Experian 1-888-397-3742 www.experian.com
- TransUnion 1-800-888-4213 www.transunion.com

Fraud Alert or Security Freeze

You have the right to place a "fraud alert" on your file at no cost. A 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.

As an alternative to a fraud alert, 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 fraud alert or security freeze as protection, please contact one of the major consumer reporting agencies listed above. That company must tell the other two:

In order to process this request, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
- 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.

Monitoring

Monitoring companies offer a variety of services ranging from alerts to insurance. It would be prudent to research credit monitoring companies such as Credit Karma (which is free), Privacy Guard, Identity Guard, LifeLock, etc. to determine if one of them is a good fit for your unique individual situation.

IRS Identity Protection PIN Opt-In Program

We have taken the following information directly from IRS Publication 5367. The single largest issue we deal with each tax season is client's Social Security Numbers being used on returns that they have not filed. Often the IRS catches these

instances and they are simple clerical errors while other times it is criminals attempting to file fraudulent returns. The PIN Opt-In Program will greatly reduce the risk of fraudulent returns entering the IRS database.

About the IP PIN: The Identity Protection Personal Identification Number (IP PIN) is a 6-digit number assigned to eligible taxpayers. It helps prevent identity thieves from filing fraudulent tax returns with stolen Social Security numbers (SSNs). An IP PIN helps the IRS verify taxpayers' identities and accept their electronic or paper tax returns for processing. The IRS issues IP PINs to confirmed identity theft victims once their cases are resolved. This process is unchanged. What is new for 2020 is the expanded number of taxpayers who are not IDT victims but who are eligible to opt into the IP PIN program. These taxpayers can opt-in by using the Get an IP PIN tool on IRS.gov.

Who is eligible for the IP PIN Opt-In Program? IP PIN eligibility for taxpayers who want to opt into the program is expanding in phases. At the start of the 2020 filing season, you may opt into the program if you filed a federal return last year from Arizona, California, Colorado, Connecticut, Delaware, District of Columbia, Georgia, Florida, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, New York, North Carolina, Pennsylvania, Rhode Island, Texas and Washington. Additional locations will be eligible later in 2020.

About the IP PIN Opt-in Program: The IP PIN is a valuable tool against tax-related identity theft. Here's what you need to know before applying:

- You must pass a rigorous identity verification process.
- Only the online process is available. (The IRS) is working on alternatives.
- Spouses and dependents are eligible for an IP PIN if they can pass the identity proofing process.
- An IP PIN is valid for a calendar year.
- You must obtain a new IP PIN each year.
- The IP PIN tool is unavailable mid-November through mid-January each year.
- Correct IP PINs must be entered on electronic and paper tax returns to avoid rejections and delays.

How to Get an IP PIN: Eligible taxpayers who want an IP PIN can go to www.irs.gov/ippin to access the Get an IP PIN tool. Taxpayers who do not already have an account, must register with the IRS.

Make sure you have all the necessary identity verification items:

- Email address
- Social Security Number (SSN) or Individual Tax Identification Number (ITIN)
- Tax filing status and mailing address
- One financial account number linked to your name: Credit card – last 8 digits (no American Express, debit or corporate cards), Student loan, Mortgage or home equity loan, Home equity line of credit (HELOC), Auto loan
- Mobile phone linked to your name (for faster registration) or ability to receive an activation code by mail

See www.irs.gov/secureaccess for tips on how to successfully authenticate your identity. Once you are registered and able to access the Get an IP PIN tool, your six-digit number will be revealed to you.

Additional Resources: You may visit the FTC's website at www.ftc.gov/idtheft and www.IdentityTheft.gov or contact the FTC directly by phone at 1.877.438.4338.