Mr. Bob Ferguson
Attorney-General of Washington State
SecurityBreach@atg.wa.gov

September 30, 2016

Dear Attorney General:

I am notifying you of a breach of unsecured personal information involving 1,198 Washington residents.

On September 12, 2016, at about 6:46 pm, an unidentified third party accessed the Vaupell computer network servers using a legitimate user ID. The incursion lasted approximately 37 minutes, some portion of which was spent accessing a departmental server that contained employee personal information, including names, addresses, dates of birth, Social Security numbers and, in some instances, pay or retirement contribution information. No bank or other financial account numbers, PINs or passwords were included in the files. The personal information comprised only a small quantity of the totality of the information on the compromised servers, which are housed at Vaupell's facility in Seattle, Washington.

The intruder destroyed all of the data on the servers he or she accessed. Because the servers had been backed up (per our usual procedure) earlier that evening, we were able to recover virtually all of the destroyed data. As a result of the destruction, we are not able to determine whether he or she downloaded or copied any of the data, including the personal data, but we have no reason to believe he or she was targeting employee personal information.

The user ID used for the intrusion has been deactivated. Seattle Police are investigating the incident, and we are taking steps to review and improve our security protocols to prevent recurrence of this type of incident.

We are sending not later than October 3, 2016, written notification to the 1,198 potentially affected Washington residents in accordance with RCW 19.255.010 in substantially the same form as the enclosed document.

If you have any questions concerning this incident, please contact me at the below indicated address.

Sincerely,

Keith W. Zeiler
COO & President, Vaupell Aerospace and Defense

www.vaupell.com
VAUPELL| GROUP COMPANY OF SUMITOMO BAKELITE CO., LTD.

VAUPELL – 1144 N.W. 53RD - SEATTLE, WA 98107, USA
TEL: +1 206 784 9050 | Fax: +1 206 784 9708 | E-MAIL: INFO@VAUPELL.COM

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

October 3, 2016

[First Name] [Last Name]
[Address 1] [Address 2]
[City], [State] [Zip]

Dear Current or Former Employee:

We write to you with important information about a potential compromise of certain personal information that occurred on the evening of September 12, 2016. On that date, an unauthorized person accessed our internal network servers for approximately 37 minutes, some portion of which was spent accessing a departmental server. The drives accessible to the intruder on that server included some small number of files containing personal information, including your personal information. We have identified how the intrusion was effected and have taken steps to prevent recurrence.

Although we have no specific basis to conclude that your personal information was the target of the intrusion or was accessed in any way, the departmental server included one or more files containing one or more of your name, address, date of birth, and Social Security Number. Some records also may have included certain payroll or retirement contribution information (although no bank or other financial account numbers, PINs or passwords). For that reason, we provide you with this notice.

In an effort to protect against any potential misuse of information that may result from the compromise, Vaupell will provide you identity theft monitoring for a period of one year through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We also recommend that you contact your bank and any credit card companies immediately to notify them of the potential disclosure of your Social Security Number. Going forward, you should continue to monitor your account statements and credit reports for evidence of fraud or identity theft. You also may take the following precautions to safeguard your personal information:

- Call the toll-free numbers of any one of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.
    - **Equifax**: 1-888-766-0008 https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp; Equifax Consumer Fraud Division, PO Box 740256, Atlanta, GA 30374
    - **Experian**: 1-888-397-3742; www.experian.com; Experian Fraud Division, P.O. Box 9554, Allen, TX 75013

- **TransUnion**: 1-800-680-7289; www.transunion.com; TransUnion Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19022

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Call the Federal Trade Commission (FTC) to get more information about fraud and identity theft. The FTC operates a call center for identity theft victims where counselors tell consumers how to protect themselves and what steps to take if they become victims of identity theft.

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

- Consider placing a security freeze on your credit reports. Unlike a fraud alert, which is free and alerts creditors to employ heightened identity verification before extending new or additional credit in your name, a security freeze restricts the credit bureaus' ability to release your credit information to third parties without your permission. Security freezes are not available in every state, and may incur an additional charge.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 844-607-1703 or going to www.myidcare.com/enrollnow and using the Access Code provided below. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is January 4, 2017.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the following access code when calling or enrolling on the website, so please do not discard this letter.

Your Access Code: [ID Experts will insert]

Please call 844-607-1703 with questions about precisely what data of yours was on the server that was compromised or if you have other questions.

Vaupell understands the importance of your personal information. We take very seriously our obligation to safeguard that information and regret that this intrusion occurred. Vaupell regularly assesses our security measures to explore ways in which we might protect and improve the security of the information we maintain. This incident only serves to reinforce that commitment.

Sincerely,

Keith W. Zeiler
COO & President, Vaupell Aerospace and Defense

myIDcare™

Recommended Steps to help Protect your Information

Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

1. **Website and Enrollment.** Go to www.myidcare.com/enrollnow and follow the instructions for enrollment using your Access Code provided above. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

2. Activate the credit monitoring provided as part of your MyIDCare membership, which is paid for by Vaupell. Credit and CyberScan monitoring are included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 844-607-1703 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned a MyIDCare Recovery Advocate who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to $5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.privacy.ca.gov) 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.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.com/, Telephone: 1-919-716-6400.

Rhode Island Residents: Office of the Attorney General, 4800 Tower Hill Road, Suite 152, Wakefield, RI 02879, www.ri.gov/, Telephone 401-782-4150

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), TDD: 1-202-326-2502.