



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

April 5, 2019

VIA E-MAIL

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
Email: SecurityBreach@atg.wa.gov

Re: Notification of Data Security Incident

Dear Attorney General Ferguson:

We represent Archbright, a company headquartered in Seattle, Washington. The purpose of this letter is to notify you pursuant to Wash. Rev. Code §§ 19.255.010-020 that, on February 20, 2019, Archbright discovered that an unauthorized individual may have accessed certain personal information within its possession belonging to 1,568 Washington residents. The information involved may have included names, addresses, driver's license numbers, Social Security numbers, and limited health or medical information.

On December 18, 2018, Archbright became aware of unusual activity within its email system. In response, Archbright took immediate steps to secure the email system, launched an internal investigation, and notified law enforcement. Archbright also retained a leading forensics firm to perform an independent investigation to determine what happened, and whether any personal information may have been accessed without authorization. After an exhaustive investigation, on February 20, 2019, Archbright learned that certain personal information belonging to Washington residents was involved in the incident. Archbright then worked diligently to locate addresses in order to provide notification to the individuals whose information was potentially affected.

Archbright mailed notification letters to the affected Washington residents between April 3, 2019 and April 5, 2019 and, in so doing, provided them with information about steps they can take to help protect their personal information. Furthermore, Archbright is providing twelve months of complimentary credit and identity monitoring services to the affected Washington residents through CyberScout, LLC. Sample copies of the notification letters are attached.

Attorney General Bob Ferguson
April 5, 2019
Page 2

Archbright is committed to protecting the sensitive information in its possession. If you have any questions or need additional information relating to this matter, please do not hesitate to contact me at (720) 292-2052 or by email at Alyssa.Watzman@lewisbrisbois.com.

Very truly yours,

A handwritten signature in black ink that reads "Alyssa" followed by a stylized flourish.

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Consumer Notification Letters



<<Date>>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident that may have affected your personal information. At Archbright, the privacy and security of your personal information is extremely important to us. Therefore, although we have no evidence that your personal information has been misused, we are writing out of an abundance of caution to inform you of the incident and to advise you of steps you can take to help protect your information. In addition, we are offering you twelve (12) months of identity protection services at no cost to you.

What Happened? On December 18, 2018, Archbright discovered unusual activity within our email system. Upon discovering the activity, we took immediate steps to secure our email and network systems. We also launched an investigation and engaged a leading forensics firm to determine what happened and whether personal information had been affected by the incident. Through the forensics investigation, we learned on February 20, 2019 that an unauthorized individual may have accessed emails and/or attachments from email accounts belonging to certain of our employees and that such documents included some of your personal information.

What Information Was Involved? The information involved in this incident may have included your name, address, driver's license number, Social Security number, and/or limited medical or health information.

What Are We Doing? As soon as Archbright discovered the incident, we took the steps described above. In addition, because we take the security of all information that we have in our systems very seriously, we have also taken steps to enhance the security of our email system and network in order to minimize the likelihood of similar incidents occurring in the future. Finally, we have also reported the incident to law enforcement to prevent fraudulent activity and will cooperate with law enforcement in an attempt to hold the perpetrators accountable.

We are not aware that any potentially impacted information has been misused. We are nonetheless providing you with information about steps you can take to protect your personal information. Moreover, to help relieve concerns and restore confidence following this incident, we are providing you with access to **Single Bureau Credit Monitoring / Single Bureau Credit Report / Cyber Monitoring** services at no cost to you. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the

bureau. The cyber monitoring will review the dark web and alert you if your personally identifiable information is found online. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by CyberScout, a global leader in risk mitigation and response with extensive experience helping people who have sustained an unintentional exposure of confidential data.

To enroll in **Credit Monitoring*** services at no charge, please log on to **<https://www.myidmanager.com>** and follow the instructions provided. **When prompted please provide the following unique code to receive services: <CODE HERE.>**

For guidance with the **CyberScout** services, or to obtain additional information about these services, **please call the CyberScout help line 1-800-405-6108** and supply the fraud specialist with your unique code. You will have until <date> to enroll in the credit monitoring services.

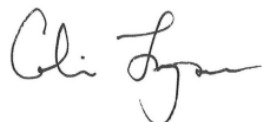
To receive these services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing your services is included with this letter.

What You Can Do: You can follow the recommendations on the following page regarding protection of personal information. We also encourage you to enroll in the free services provided by CyberScout, and to regularly review your credit report. If you see anything that you do not understand or that looks suspicious, you should contact the three consumer reporting agencies listed under the section titled "Steps You Can Take to Further Protect Your Information" for additional assistance.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call CyberScout at 1-800-405-6108 Monday through Friday from 8:00am to 5:00pm Pacific Time.

We take your trust in us and this matter very seriously and we apologize for any worry or inconvenience that this incident may cause you.

Sincerely,



Colin Lyons
Director, IT and Business Intelligence
Archbright

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
--	---	---	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400
---	--	--	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



<<Date>>

Family of

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

Subject: Notice of Data Security Incident

Dear Family of <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident that may have affected your deceased family member’s personal information. At Archbright, the privacy and security of personal information is extremely important to us. Therefore, although we have no evidence that your deceased family member’s personal information has been misused, we are writing out of an abundance of caution to inform you of the incident and to advise you of steps you can take to help protect their information

What Happened? On December 18, 2018, Archbright discovered unusual activity within our email system. Upon discovering the activity, we took immediate steps to secure our email and network systems. We also launched an investigation and engaged a leading forensics firm to determine what happened and whether personal information had been affected by the incident. Through the forensics investigation, we learned on February 20, 2019 that an unauthorized individual may have accessed emails and/or attachments from email accounts belonging to certain of our employees and that such documents included some of your deceased family member’s personal information.

What Information Was Involved? The information involved in this incident may have included your deceased family member’s name, address, driver’s license number, Social Security number, and/or limited medical or health information.

What Are We Doing? As soon as Archbright discovered the incident, we took the steps described above. In addition, because we take the security of all information that we have in our systems very seriously, we have also taken steps to enhance the security of our email system and network in order to minimize the likelihood of similar incidents occurring in the future. Finally, we have also reported the incident to law enforcement to prevent fraudulent activity and will cooperate with law enforcement in an attempt to hold the perpetrators accountable.

We are not aware that any potentially impacted information has been misused. We are nonetheless providing you with information about steps you can take to protect your deceased family member’s personal information. Moreover, to help relieve concerns and restore confidence following this incident, we are providing you with access to **Cyber Monitoring** services at no cost to you. The cyber monitoring will review the dark web and alert you if your

deceased family member's personally identifiable information is found online. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you would like help with placing a Credit File Death Suppression. These services will be provided by CyberScout, a global leader in risk mitigation and response with extensive experience helping people who have sustained an unintentional exposure of confidential data.

To enroll in **Cyber Monitoring*** services at no charge, please log on to **<https://www.myidmanager.com>** and follow the instructions provided. **When prompted please provide the following unique code to receive services: <CODE HERE.>**

For guidance with the **CyberScout** services, or to obtain additional information about these services, **please call the CyberScout help line 1-800-405-6108** and supply the fraud specialist with the unique code referenced above. You will have until <date> to enroll in the monitoring services.

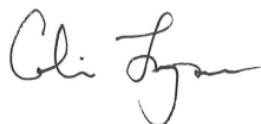
To receive these services, you must have a Social Security number in your deceased family member's name, and have a U.S. residential address associated with their credit file. Additional information describing services is included with this letter.

What You Can Do: You can follow the recommendations on the following page regarding protection of personal information. We also encourage you to enroll deceased family member in the free services provided by CyberScout. If you see anything that you do not understand or that looks suspicious, you should contact the three consumer reporting agencies listed under the section titled "Steps You Can Take to Further Protect Your Information" for additional assistance.

For More Information: Further information about how to protect your deceased family member's personal information appears on the following page. If you have questions or need assistance, please call CyberScout at 1-800-405-6108 Monday through Friday from 8:00am to 5:00pm Pacific Time.

We take your trust in us and this matter very seriously and we apologize for any worry or inconvenience that this incident may cause you.

Sincerely,



Colin Lyons
Director, IT and Business Intelligence
Archbright

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
--	---	---	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400
---	--	--	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



<<Date>>

Parent or Guardian of

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

Subject: Notice of Data Security Incident

Dear Parent or Guardian of <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident that may have affected your child's personal information. At Archbright, the privacy and security of personal information is extremely important to us. Therefore, although we have no evidence that your child's personal information has been misused, we are writing out of an abundance of caution to inform you of the incident and to advise you of steps you can take to help protect their information.

What Happened? On December 18, 2018, Archbright discovered unusual activity within our email system. Upon discovering the activity, we took immediate steps to secure our email and network systems. We also launched an investigation and engaged a leading forensics firm to determine what happened and whether personal information had been affected by the incident. Through the forensics investigation, we learned on February 20, 2019 that an unauthorized individual may have accessed emails and/or attachments from email accounts belonging to certain of our employees and that such documents included some of your child's personal information.

What Information Was Involved? The information involved in this incident may have included your child's name, address, driver's license number, Social Security number, and/or limited medical or health information.

What Are We Doing? As soon as Archbright discovered the incident, we took the steps described above. In addition, because we take the security of all information that we have in our systems very seriously, we have also taken steps to enhance the security of our email system and network in order to minimize the likelihood of similar incidents occurring in the future. Finally, we have also reported the incident to law enforcement to prevent fraudulent activity and will cooperate with law enforcement in an attempt to hold the perpetrators accountable.

We are not aware that any potentially impacted information has been misused. We are nonetheless providing you with information about steps you can take to protect your child's personal information. Moreover, to help relieve concerns and restore confidence following this incident, we are providing the parents of impacted minor dependents with access to **Cyber Monitoring*** services at no charge. The cyber monitoring will review the dark web and alert you

if your child's personally identifiable information is found online. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you would like help with a Protected Consumer Credit File Freeze. These services will be provided by CyberScout, a global leader in risk mitigation and response with extensive experience helping people who have sustained an unintentional exposure of confidential data.

To enroll in **Cyber Monitoring*** services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. **When prompted please provide the following unique code to receive services:** <CODE HERE.>

For guidance with the **CyberScout** services, or to obtain additional information about these services, **please call the CyberScout help line 1-800-405-6108** and supply the fraud specialist with your child's unique code. You will have until <date> to enroll in the credit monitoring services.

To receive these services, your child must have a Social Security number in their name, and have a U.S. residential address associated to them. Additional information describing your child's services is included with this letter.

What You Can Do: You can follow the recommendations on the following page regarding protection of personal information. We also encourage you to enroll your child in the free services provided by CyberScout, and to regularly contact the credit bureaus and ensure that no credit file exists in the name of your minor child. If you see anything that you do not understand or that looks suspicious, you should contact the three consumer reporting agencies listed under the section titled "Steps You Can Take to Further Protect Your Information" for additional assistance.

For More Information: Further information about how to protect your child's personal information appears on the following page. If you have questions or need assistance, please call CyberScout at 1-800-405-6108 Monday through Friday from 8:00am to 5:00pm Pacific Time.

We take your trust in us and this matter very seriously and we apologize for any worry or inconvenience that this incident may cause you.

Sincerely,



Colin Lyons
Director, IT and Business Intelligence
Archbright

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
--	---	---	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400
---	--	--	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.