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>>

Dear <<Name 1>>:

We are sending this letter to you as part of Fairbanks North Star Borough's commitment to patient privacy to inform you of a data security incident that may have affected your personal information. The Borough's former billing vendor for ambulance Emergency Medical Services ("EMS"), Golden Heart Administrative Professionals, Inc. ("GHAP"), reported to the Borough that GHAP experienced a cybersecurity incident and that certain information within GHAP's computer system was compromised.

The following details of the incident have been provided by GHAP:

GHAP's Description of the Incident: GHAP was the Borough's emergency medical services ("EMS") ambulance billing agency from 2012 through 2017. The Borough switched billing service providers in 2017. Based on the information provided to us by GHAP, we understand that GHAP was subject to a ransomware attack that resulted in the encryption of certain information maintained in its computer system. Upon discovery of the incident, GHAP retained a third-party IT and forensics firm to investigate the incident. According to GHAP, the forensic investigation determined that all information in the GHAP system was potentially compromised and subject to the unauthorized access and acquisition by an unknown third-party, including affected individuals' names, addresses, Social Security numbers, dates of birth, medical treatment and diagnosis codes and, in certain instances where payment was made by credit card, credit card information and other potentially sensitive information.

Date of Incident and GHAP's Notification to the Borough: GHAP reported that the ransomware attack occurred on April 14, 2018, and that the attack was discovered by GHAP on that same day. As described further, below, GHAP has taken steps to minimize the impact of the incident. GHAP provided an initial notification of the incident to the Borough in a letter, dated May 25, 2018. However, GHAP did not provide detailed information concerning the incident or who was affected until June 18, 2018.

What you can do to protect yourself: Out of an abundance of caution, we are offering a complimentary one-year membership in Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

Steps taken by GHAP and the Borough: We have been advised by GHAP that it is working with its technology service provider to mitigate any further damage as a result of this incident and to increase the security of its system to provide protection against future cyber-attacks. GHAP has advised us that it has notified law enforcement of the incident as well as the three major credit agencies (Equifax, Experian, and TransUnion). Additionally, we have been advised by GHAP that it has replaced the affected computer hardware and installed updated computer software on its systems, is re-evaluating the security of its computer system and will provide updated training to its personnel. We will continue to monitor GHAP's investigation and will work with our current ambulance billing provider to ensure that it has adequate administrative, technical and physical safeguards to protect personal information against similar future threats.

We value the trust you place in us to protect the privacy and security of your personal information, and we apologize for any inconvenience or concern that this incident might cause you. The Borough is committed to keeping your information safe and recognizes the importance of securing your healthcare and financial information.

If you have any additional questions, you may call our confidential inquiry line at 1-888-668-9006, between 5 a.m. and 5 p.m., Alaska Time, Monday through Friday.

Sincerely,

Wendy Tisland
Risk Manager
Fairbanks North Star Borough

Activating Your Complimentary Credit Monitoring

To help protect your identity, we are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<Enrollment Deadline>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code: <<Activation Code>>**

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 877-288-8057. Be prepared to provide engagement number **<<Engagement #>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian Identity Works, you will have access to the following additional features:

- **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, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the Activation Code listed above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

Additional Important Information
As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your credit card 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 incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, 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 print a copy of the request form at www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: 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 ninety (90) days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788	P.O. Box 9554	Fraud Victim Assistance Department
Atlanta, GA 30348	Allen, TX 75013	P.O. Box 2000
		Chester, PA 19016

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines IA 50319
515-281-5164

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at:

Office of the Attorney General
220 St. Paul Place
Baltimore, MD 21202
(888) 743-0023

New Mexico Residents: New Mexico residents can obtain information about preventing identity theft the New Mexico Attorney General's Office at

Office of the Attorney General
408 Galisteo Street
Villagra Building
Santa Fe, NM 87501
(505) 490-4060

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226

Rhode Island Residents: We believe that this incident affected one (1) Rhode Island resident. Rhode Island residents can contact the Office of the Attorney general at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400

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

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

<<Date>>

Dear Administrator/Executor of the Estate of <<Name1>>:

We are sending this letter to you as part of Fairbanks North Star Borough's commitment to patient privacy to inform you of a data security incident that may have affected your deceased relative's personal information. The Borough's former billing vendor for ambulance Emergency Medical Services ("EMS"), Golden Heart Administrative Professionals, Inc. ("GHAP"), reported to the Borough that GHAP experienced a cybersecurity incident and that certain information within GHAP's computer system was compromised.

The following details of the incident have been provided by GHAP:

GHAP's Description of the Incident: GHAP was the Borough's emergency medical services ("EMS") ambulance billing agency from 2012 through 2017. The Borough switched billing service providers in 2017. Based on the information provided to us by GHAP, we understand that GHAP was subject to a ransomware attack that resulted in the encryption of certain information maintained in its computer system. Upon discovery of the incident, GHAP retained a third-party IT and forensics firm to investigate the incident. According to GHAP, the forensic investigation determined that all information in the GHAP system was potentially compromised and subject to the unauthorized access and acquisition by an unknown third-party, including affected individuals' names, addresses, Social Security numbers, dates of birth, medical treatment and diagnosis codes and, in certain instances where payment was made by credit card, credit card information and other potentially sensitive information.

Date of Incident and GHAP's Notification to the Borough: GHAP reported that the ransomware attack occurred on April 14, 2018, and that the attack was discovered by GHAP on that same day. As described further, below, GHAP has taken steps to minimize the impact of the incident. GHAP provided an initial notification of the incident to the Borough in a letter, dated May 25, 2018. However, GHAP did not provide detailed information concerning the incident or who was affected until June 18, 2018.

Steps taken by GHAP and the Borough: We have been advised by GHAP that it is working with its technology service provider to mitigate any further damage as a result of this incident and to increase the security of its system to provide protection against future cyber-attacks. GHAP has advised us that it has notified law enforcement of the incident as well as the three major credit agencies (Equifax, Experian, and TransUnion). Additionally, we have been advised by GHAP that it has replaced the affected computer hardware and installed updated computer software on its systems, is re-evaluating the security of its computer system and will provide updated training to its personnel. We will continue to monitor GHAP's investigation and will work with our current ambulance billing provider to ensure that it has adequate administrative, technical and physical safeguards to protect personal information against similar future threats.

What you can do to protect your deceased relative: While credit monitoring and identity theft protection services are not available for deceased individuals, there are steps you can take to request a copy of your deceased relative's credit report. An executor or surviving spouse can place a request to any of the three national credit reporting agencies for a copy of the deceased individual's credit report along with making one of the following notations:

- "Deceased" – Do not issue credit"; or
- "If an application is made for credit, please notify the following person(s): (e.g., list a surviving relative, executor/trustee of the estate, and/or local law enforcement agency —noting the relationship to the deceased individual)."

Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your deceased relative's credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your relative's credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016

For more information regarding identity theft and the deceased, please visit http://www.idtheftcenter.org and search for "FS 117 – Identity Theft and the Deceased – Prevention and Victim Tips." You may wish to review the tips provided by the Federal Trade Commission ("FTC") on how to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

We value the trust you place in us to protect the privacy and security of your deceased relative's personal information, and we apologize for any inconvenience or concern that this incident might cause you. The Borough is committed to keeping personal information safe and recognizes the importance of securing healthcare and financial information.

If you have any additional questions, you may call our confidential inquiry line at 1-888-668-9006, between 5 a.m. and 5 p.m., Alaska Time, Monday through Friday.

Sincerely,

Wendy Tisland

Wendy Tisland
Risk Manager
Fairbanks North Star Borough