August 29, 2018

«First» «Last»
«Address_1» «Address_2»
«City_State_Zip»

Dear «First»:

Gray respects and at all times seeks to protect the privacy and security of the personal information it maintains on behalf of our team members. This is why, as a precautionary measure, we are writing to you with important information about an unauthorized disclosure that involved your personal information.

What happened
On August 17, an internal technical support call revealed emails sent to a Gray team member beginning April 1st, *containing team member personal information*, had been automatically forwarded to an unknown g-mail account by way of that team member's email having been "hacked." Information that was forwarded may have included team members' names, addresses and in some cases banking and social security numbers. No personal health information was disclosed.

The potential breach is internal to Gray and does not impact the security and integrity of any of our outside provider websites including Anthem, Delta Dental, HSA Bank, or Transamerica.

What we are doing
Gray immediately initiated an investigation and have enlisted the assistance of cybersecurity professionals to assess the incident and to work with our team to prevent or mitigate any harm that could come from the unauthorized access. In addition, we reported this matter to the appropriate authorities. As of today, we have an external forensic cybersecurity team continuing to investigate and we will keep team members apprised as new information becomes available. Additionally, we have put new procedures in place to better secure the access to personal information and will continue to evaluate and improve those as rapidly as possible.

At this point, we do not have any indication that your personal data has been misused in any way and are constantly monitoring all indicators. Please keep in mind this is an on-going investigation and as additional information becomes available we will be communicating this directly to team members. Should you have any questions and concerns about the loss of your personal information, please contact Shawn Fister at (859) 281-9208 or sfister@gray.com or Brian Silver at BSilver@gray.com.

What you should do
As discussed above, Gray believes that the unauthorized disclosure was limited to the information described above. However, in any situation involving personal information, we encourage you to review your accounts for any suspicious activity. In addition, you may want to consider changing your account passwords to further protect your personal information.

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 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service: PO Box 105281 Atlanta, GA 30348.

Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below.

- **Equifax:** 1-800-525-6285; www.equifax.com; PO Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; PO Box 9532, Allen, TX 75013
- **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790.

When you receive your credit reports review them for: accounts you did not open, inquiries from creditors you did not initiate, personal information, which is not accurate, etc. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

To help ensure that your personal information is not used inappropriately, 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 before opening any accounts in your name. You may also want to review the tips provided by the Federal Trade Commission on how to avoid identity theft at http://www.ftc.gov/idtheft or by calling 1-877-ID-THEFT (877-438-4338). A copy of "Take Charge: Fighting Back against Identity Theft," can be found on the FTC's website at www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

Our commitment to you

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll Breach Response Services to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include:

Credit Report and Credit Monitoring

Credit reports and monitoring deliver real-time insight into credit activity to detect suspicious activity that could be linked to identity theft. All services can be accessed via Kroll's online web portal. Credit services are backed by Kroll's team of Licensed Fraud Investigator.

Web Watcher Internet Monitoring

Kroll offers an Internet fraud monitoring service for events involving information not directly related to credit. Web Watcher monitors thousands of identity trading websites, chat rooms, forums and networks for personal information including: SSN, credit card numbers, emails, phone numbers, bank account and routing numbers, etc. Web Watcher is backed by Kroll's team of Licensed Fraud Investigators.

Public Persona

Monitors and notifies when unauthorized names, aliases and addresses become associated with an individual's Name and Date of Birth. Public Persona monitors public records including; real estate data, new mover information, property and recorder of deed registration, internet job site providers, state occupational license data providers, voter information, court proceedings, bankruptcies, liens and judgments.

Quick Cash Scan

Monitors 21,000 online, rent-to-own, and payday lender storefronts for unauthorized activity. An initial report is provided and monitoring is provided monthly. An alert will be generated when new loans or inquiries are detected.

Identity Theft Insurance

Identity Theft Insurance will reimburse for expenses associated with restoring one's identity should they become a victim of identity theft. If an identity is compromised, the carrier provides coverage for up to USD $1,000,000, from an A.M. Best "A-rated" carrier.

How to Activate Your Credit and Identity Monitoring Services

1. You must activate your identity monitoring services by November 25, 2018. Your Activation Code will not work after this date.
2. Visit **redeem.kroll.com** to activate your identity monitoring services.
3. Provide Your Activation Code: **«Code_Sent»** and Your Verification ID: **3VY**
4. To sign in to your account after you have activated your identity monitoring services, please visit **krollbreach.idmonitoringservice.com**

If you have questions, please call 1-866-775-4209, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. I personally apologize for the stress and worry this incident may cause you and can assure you we are doing everything we can to rectify the situation.

Sincerely,

Stephen A. Gray
President & Chief Executive Officer