



Dear Attorney General Frosh,

Feldesman Tucker Leifer Fidell (FTLF) represents Rosemount Center, Inc. (Rosemount), a DC-based non-profit organization providing early childhood education and family support services to pregnant women, infants, toddlers and preschool-aged children and their families. On behalf of Rosemount, I am submitting this notification of a business email compromise that affected the personally identifiable information of one Maryland resident.

1. Brief description of the nature of the security incident:

On June 21, 2022, Rosemount discovered that funds from its bank account were transferred without appropriate authorization. Rosemount immediately contacted the bank, law enforcement and its IT Team. A preliminary incident summary by the IT Team determined that a threat actor initially gained access to an employee's email account on May 17 and then used the compromised email account to communicate with the bank to initiate the fraudulent wire transfer. The bank recovered nearly all the funds and returned them to Rosemount.

On June 30, FTLF retained a forensic investigator to investigate the scope of the incident. On August 21, the external forensic investigator provided its report. The report provided the details necessary for FTLF to advise Rosemount on the required notifications, including providing this notice to the Maryland Attorney General's Office and the notice sent to the affected Maryland resident.

2. Number of Maryland residents being notified: 1.

3. Information compromised: Name, Social Security number, date of birth, and driver's license number.

4. Any steps the business is taking to restore the integrity of the system:

On June 21, Rosemount's IT Team blocked unauthorized access to the compromised email account. On June 22, Rosemount's IT Team began to remediate the incident. Since the security incident, Rosemount has implemented multifactor authentication for Office 365 users. Rosemount has also upgraded its anti-virus and anti-malware protections, including adding email spam and business email protection and reporting. Rosemount has also launched new security awareness training which is required for all staff members.

As described in the attached notice to the affected Maryland resident, Rosemount offered to reimburse them for the cost of 18 months of identity theft prevention services. Rosemount also provided details on reviewing credit reports, placing fraud alerts and placing a security freeze. Rosemount also provided contact information for the Federal Trade Commission and the Office of the Attorney General of Maryland.

Should you have any questions or require any additional information, please contact me at dpledgie@ftlf.com or 202-466-0954.

Take good care,
~dkp

Dianne K. Pledgie she/her/hers
Partner and Compliance Counsel
Feldesman Tucker Leifer Fidell LLP
1129 20th Street, NW, Suite 400
Washington, DC 20036
T. 202.466.8960
F. 202.293.8103

www.ftlf.com

FELDESMAN + TUCKER + LEIFER + FIDELL LLP

CONFIDENTIALITY NOTICE: This e-mail and any attachments contain information from the law firm of Feldesman Tucker Leifer Fidell LLP and are intended solely for the use of the individual or entity named in the e-mail. If you have received this e-mail in error, notify DPledgie@feldesmantucker.com immediately and delete the e-mail, any attachments, and any copies of the e-mail or attachments.

Dianne K. Pledge dpledgie@ftlf.com

September 20, 2022

Dear [Resident],

I am writing on behalf of Rosemount Center, Inc. ("Rosemount"), to inform you about a recent security incident that involved your personally identifiable information.

What happened: On June 21, 2022, Rosemount discovered that funds from its bank account were transferred without appropriate authorization. Rosemount immediately contacted the bank and law enforcement. Rosemount's IT Team launched an internal investigation and determined that on May 17, 2022, the email account of a Rosemount employee was first accessed by the threat actor. The compromised account was used to initiate the fraudulent wire transfer.

On June 30, an outside forensic investigator was hired to determine the scope of the security incident. On August 21, the outside forensic investigator provided its final report. You are receiving this letter because your personally identifiable information was affected by this security incident.

What information was involved: The following personal information was involved in this security incident: your name, Social Security number, date of birth, and driver's license number.

What we are doing: Rosemount immediately reported the security incident to the bank and law enforcement. Since the security incident, Rosemount has worked to improve the security of its systems, including implementing multi-factor authentication, increasing anti-virus and anti-malware protections, and requiring additional security awareness training for staff members.

What you can do:

- **Enroll in credit monitoring:** We recommend that you enroll in credit monitoring. Rosemount will reimburse you for the cost of 18 months of identity

theft prevention services. To learn more, please contact Eileen Gaffigan at 202-265-9885, ext. 121, or at egaffigan@rosemountcenter.com.

- **Review your credit reports:** We recommend that you remain vigilant by reviewing your account statements and monitoring credit reports. Under federal law, you are entitled to one free copy of your credit report from each of the three major credit reporting companies every 12 months. To obtain a free annual credit report, visit www.annualcreditreport.com or call 1-877-322-8228; TTY: 1-877-730-4204.

If you experience identity fraud, you have the right to file a police report. To file a crime report or incident report with law enforcement for identity theft, you will likely need to provide 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.

- **Place fraud alerts:** 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 may also delay you when you seek to obtain credit. You can place a fraud alert by contacting one of the three major credit agencies directly at:

Experian	Equifax	TransUnion
P.O. Box 4500	P.O. Box 740241	P.O. Box 2000
Allen, TX 75013	Atlanta, GA 30374	Chester, PA 19016
www.experian.com	www.equifax.com	www.transunion.com
1-888-397-3742	1-800-525-6285	1-800-680-7289

You only need to contact 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. 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. An initial fraud alert lasts one year.

- **Place a 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 to place the freeze. 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. There is no cost to freeze or unfreeze your credit files.

- **Obtain additional information:** 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. Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.consumer.gov/idtheft, Telephone: 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.
 - 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.

If you have questions or concerns, please contact me at 800-266-1938 or at dpledger@ftlf.com.

Sincerely,

Dianne K Pledgie, Esq.
Partner
Feldesman Tucker Leifer Fidell