Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 11, 2022

i1862-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 EMPLOYEE
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Dear Sample A. Sample:

Re: Notice of Data Incident

We are writing to provide you with additional information about the systems outage we previously communicated with you about. This letter explains what happened, what information may have been affected, what measures we are taking in response, and steps you can take to protect yourself.

What Happened
We discovered that our systems were experiencing an issue that prevented employees from accessing certain systems and servers on October 24, 2021. In response, we immediately launched an internal investigation and engaged outside expert consultants. At the same time, we took proactive measures to contain and mitigate the systems issue, including by taking our network and computers down. We also contacted law enforcement and cooperated with them in their investigation.

From our in-depth investigation, supported by our external experts, we discovered the systems outage was caused by a cyber-attack that encrypted some network servers. Based on this investigation, we recently discovered that the attack may have impacted your personal information. Our investigation has not revealed evidence of fraudulent data use. However, we want to provide you with information you can use to proactively take steps to protect yourself and your information.

What Information Was Involved
Our in-depth investigation has revealed that certain network servers and systems were encrypted during the attack. Some of these encrypted systems held, among other things, electronic files which contained certain of your personal information. As a result, we believe it is possible that the encryption event may have incidentally impacted personal information that we maintain about you. Which specific information of yours was impacted depends on the data we maintain about you, but may have included: name, social security number, driver's license number, passport number, financial account information, medical information and date of birth.

What We Are Doing
As noted, as soon as we discovered the systems issue, we immediately launched an internal investigation and engaged the assistance of outside forensic experts and experienced cyber-consultants. At the same time, we took proactive measures to contain and mitigate the systems issue, including by taking certain aspects of our network and computers down. We have also worked to restore our systems from back-up servers unaffected by the systems outage, have reset all network administrative credentials and passwords, have been performing ongoing additional forensic scans on our systems, and are conducting regular testing, patching, training and other steps to further protect our networks. We also contacted law enforcement and have been cooperating with them in their investigation of the attack.

We take this matter very seriously, and in addition to the steps already described, Valent is offering you 24 months of **free** fraud detection and identity theft protection. If you wish to take advantage of these services, activation instructions are below.

What You Can Do
We encourage you to remain vigilant by reviewing your account statements and credit reports closely. At the end of this letter, we have provided you with additional information regarding steps you can proactively take to further protect yourself and your personal information. It describes information about (1) reporting suspicious activity or suspected identity theft, (2) credit reports, (3) fraud alerts, (4) credit/security freezes, (5) your rights under the Fair Credit Reporting Act, and (6) information about taxes. We encourage you review that additional information.

Free Credit Monitoring and Identity Theft Protection: Even though we have no evidence that your personal information has been fraudulently used or publicly disclosed, as a precautionary measure, we are offering to provide you with 24 months of free identity monitoring, fraud consultation, and identity theft restoration services through Experian's IdentityWorks™ product. To take advantage of these free services, please follow the steps below:

- Ensure that you enroll by October 31, 2022. Your code will not work after this date.
- Visit the Experian IdentityWorks™ website to enroll: https://www.experianidworks.com/credit
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, please contact Experian's customer care team at (877) 653-0568 by October 31, 2022. Be prepared to provide engagement number B058629 as proof of eligibility for the identity restoration services by Experian.

For More Information
We take very seriously the security and privacy of your information, and deeply regret any inconvenience this may cause. If you have any questions, please call (877) 653-0568 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B058629.

Sincerely,

Matt Plitt
CEO, Valent U.S.A. LLC

4600 Norris Canyon Road
San Ramon, CA 94583

Additional Steps You Can Take to Protect Your Personal Information

Report Suspicious Activity or Suspected Identity Theft. If you detect any unauthorized or suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. If you suspect any identity theft has occurred, you can contact your local law enforcement by filing a police report or the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT (1-877-438-4338), by writing to the FTC at 600 Pennsylvania Avenue, NW Washington DC 20580, or online at www.ftc.gov. You can also contact your state Attorney General (information for some specific AGs is listed below):

- Maryland residents may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us, by sending an email to idtheft@oag.state.md.us, or by calling 410-576-6491.

- New York residents may wish to review information on security breach response and identity theft prevention and protection information provided by the New York Attorney General at https://ag.ny.gov/internet/privacy-and-identity-theft or by calling 1-800-771-7755 and by the New York Department of State, Division of Consumer Protection at https://dos.ny.gov, or by calling 800-697-1220.

- North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov/, by calling 877-566-7226, or by writing to 9001 Mail Service Center, Raleigh, NC 27699.

Contacting the Internal Revenue Service: If you believe you are the victim of tax fraud or that somebody has filed or accessed your tax information, you should immediately contact the IRS or state tax agency as appropriate. For the IRS, you can use Form 14039 (https://www.irs.gov/pub/irs-pdf/f14039.pdf). You can also call them at 800-908-4490 (Identity Theft Hotline). Information on how to contact your state department of revenue to make similar reporting may be found by going to http://www.taxadmin.org/state-tax-agencies.

Credit Reports/Fraud Alerts/Credit and Security Freezes: Under federal law, you are entitled to one free copy of your credit report every 12 months. You can request a free credit report once a year at www.annualcreditreport.com, by calling (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. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

As a precautionary step, to protect yourself from possible identity theft you can place a fraud alert on your bank accounts and credit file. A fraud alert tells creditors to follow certain procedures before opening a new account in your name or changing your existing account. You may call any one of the three major credit bureaus listed below to place a fraud alert on your file. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. All three credit reports will be sent to you, free of charge, for your review.

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. 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 apply for a new credit card, loan, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze on your file you may be required to provide the consumer reporting agency with information that identifies you including your Social Security Number. There may be a fee for this service based on state law (in MA, there shall be no charge). To put a security freeze on your credit file contact the consumer reporting agencies listed below.

You also contact the three U.S. credit reporting agencies as follows:

Agency	Credit Report Contact	Fraud Alert Contact	Credit/Security Freeze Contact
TransUnion LLC	TransUnion LLC Consumer Disclosure Center, P.O. Box 1000, Chester, PA 19016; (800) 888-4213; https://www.transunion.com	TransUnion Fraud Victim Assistance, P.O. Box 2000, Chester, PA 19016; (800) 680-7289; https://www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 160, Woodlyn, PA 19094; (888) 909-8872; https://www.transunion.com/credit-freeze/
Experian	P.O. Box 2002, Allen, TX 75013; (888) 397-3742; https://www.experian.com/consumer-products/free-credit-report.html	Experian, P.O. Box 9554, Allen, TX 75013; (888) 397-3742; https://www.experian.com/fraud/center.html	P.O. Box 9554, Allen, TX 75013; (888) 397-3742; https://www.experian.com/freeze/center.html
Equifax Information Services LLC	Equifax Information Services LLC, P.O. Box 740241, Atlanta, GA 30374; (866) 349-5191; https://www.equifax.com/personal/credit-report-services/	Equifax Information Services LLC, P.O. Box 105069, Atlanta, GA 30348-5069; (800) 525-6285; https://www.equifax.com/personal/credit-report-services/	Equifax Information Services LLC, P.O. Box 105788, Atlanta, GA 30348-5788; (888) 298-0045 or (800) 349-9960; https://www.equifax.com/personal/credit-report-services/

Federal Fair Credit Reporting Act rights: You have rights under the federal Fair Credit Reporting Act that include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. More information about your rights is at www.ftc.gov.

***IRS Identity Protection PIN*:** The IRS offers an Identity Protection PIN, which is a six digit number that prevents someone else from filing a tax return using your Social Security number. The Identity Protection PIN is known only to you and the IRS. For more information and to obtain an Identity Protection PIN, please visit the IRS website at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.