



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

J5547-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 GENERAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



June 12, 2023

RE: Important Security Notification. Please read this entire letter.

Dear Sample A. Sample:

I'm writing on behalf of Commonwealth Health Physician Network-Cardiology, also known as Great Valley Cardiology or GVC. We sincerely regret to report that GVC experienced a security incident that may have exposed your personal information.

On April 13, 2023, GVC became aware that unauthorized parties might have access to the GVC computer network. GVC disconnected the GVC computer network from the internet, disabled VPN access, and immediately opened an investigation. The unauthorized parties no longer have access to the GVC network. GVC has also been in contact with law enforcement.

GVC's investigation determined that between February 2, 2023 and April 14, 2023, unauthorized parties bypassed GVC security measures and gained access to the GVC network. Our investigation showed they had access to files on the GVC network that included your personal information, including your name, address, [Extra1].

We cannot determine whether the unauthorized parties viewed or took the personal information to which they had access. To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months. A credit card is not required for enrollment in Experian IdentityWorks. To start monitoring your personal information:

- Ensure that you enroll by **September 30, 2023** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/plus>.
- Provide your **activation code**:

0000001



You will have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related 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.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please contact an Experian agent. After it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

If you have questions about Experian IdentityWorks, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **833-901-4624** 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) by September 30, 2023. Be prepared to provide engagement number **B096381** as proof of eligibility for the Identity Restoration services by Experian.

We are committed to the privacy of your personal information and regret any inconvenience this incident may cause.

Sincerely,



Erik Schab
Director of Operations
Great Valley Cardiology

*The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

What else can you do to protect your personal information?

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

Order your free credit report at annualcreditreport.com, call toll-free at [877-322-8228](tel:877-322-8228), or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. You have rights under the federal Fair Credit Reporting Act (FCRA). These 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.

Place a fraud alert on your credit file. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a security freeze on your credit file, which generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

- **Equifax**[®]
P.O. Box 740256
Atlanta, GA 30374
[1-800-525-6285](tel:1-800-525-6285)
www.equifax.com
- **Experian**[®]
P.O. Box 9554
Allen, TX 75013
[1-888-397-3742](tel:1-888-397-3742)
www.experian.com
- **TransUnion**[®]
P.O. Box 2000
Chester, PA 19016
[1-800-680-7289](tel:1-800-680-7289)
www.transunion.com

Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

If you aren't already doing so, please pay close attention to all bills and credit card charges you receive for items you did not contract for or purchase. Review all your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

The FTC offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the FTC. You can learn more about how to protect yourself from becoming an identity theft victim by contacting the FTC at 877.IDTHEFT ([1-877-438-4338](tel:1-877-438-4338)), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.



For District of Columbia Residents: You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, [202.727.3400](tel:202.727.3400), oag.dc.gov.

For Maryland Residents: You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888.743.0023, <https://www.marylandattorneygeneral.gov/>.

For New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These 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. For more information about the FCRA, please visit ftc.gov.

In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have the right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about obtaining a security freeze, go to <https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts>.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, [212-416-8433](tel:212-416-8433) or <https://ag.ny.gov/resources/individuals/credit-lending/identity-theft>; or 2) NYS Department of State's Division of Consumer Protection, [800-697-1220](tel:800-697-1220) or <https://dos.ny.gov/consumer-protection>.

For North Carolina Residents: You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, [1-877-566-7226](tel:1-877-566-7226), ncdoj.gov.

For Rhode Island Residents: You have the right to obtain a copy of the applicable police report, if any, relating to this incident. You may contact and obtain information from and/or report identity theft to your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street Providence, RI 02903; Phone: [401-274-4400](tel:401-274-4400); Website: www.riag.ri.gov



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

J5547-L05-0000002 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L05 DESCENDANT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



June 12, 2023

RE: Important Security Notification. Please read this entire letter.

To the Next of Kin/Estate of Sample A. Sample:

I’m writing on behalf of Commonwealth Health Physician Network-Cardiology, also known as Great Valley Cardiology or GVC. We sincerely regret to report that GVC experienced a security incident that may have exposed the personal information of the patient listed above. We are writing to you in your role as the next of kin or personal representative of the patient’s estate.

On April 13, 2023, GVC became aware that unauthorized parties might have access to the GVC computer network. GVC disconnected the GVC computer network from the internet, disabled VPN access, and immediately opened an investigation. The unauthorized parties no longer have access to the GVC network. GVC has also been in contact with law enforcement.

GVC’s investigation determined that between February 2, 2023 and April 14, 2023, unauthorized parties bypassed GVC security measures and gained access to the GVC network. Our investigation showed they had access to files on the GVC network that included the patient’s personal information, including name, address, [Extra1].

We cannot determine whether the unauthorized parties viewed or took the personal information to which they had access. We do not want this incident to pose a risk of identity theft. The attached sheet provides precautionary measures you can take to protect the patient’s personal information, including notifying one of the nationwide credit bureaus about the patient’s death, which will cause a death notice to be placed on their credit reports. A death notice flags a person’s credit reports as “deceased – do not issue credit.” Additionally, you should remain vigilant in reviewing the patient’s financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

0000002



If you have further questions or concerns, please call **833-901-4624** 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 this Experian engagement number: **B096383**.

We are committed to the privacy of our patients' personal information and regret any inconvenience this incident may cause.

Sincerely,

A handwritten signature in black ink that reads "Erik Schab". The signature is written in a cursive, flowing style.

Erik Schab
Director of Operations
Great Valley Cardiology

What else can you do to protect the decedent's personal information?

We recommend you remain vigilant and consider taking the following steps to protect the decedent's personal information:

Order a free credit report at annualcreditreport.com, call toll-free at 877.322.8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov. When you receive the decedent's credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in the decedent's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

If you have not already done so, you can also request the three credit bureaus to place the following alert in the decedent's file:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

Here is the contact information for the three credit bureaus:

Equifax
P.O. Box 740256
Atlanta, GA 30374
800-525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com

Remove the decedent's name from mailing lists of pre-approved offers of credit.

Pay close attention to all bills and credit card charges you receive and check for items the decedent did not purchase. Review all bank account statements frequently for checks, purchases, or deductions not made by the decedent or you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically because identity thieves sometimes hold on to stolen personal information before using it.

The FTC offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the FTC. You can learn more about how to protect the decedent and yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 877.IDTHEFT (1.877.438.4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

For District of Columbia Residents: You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, [202.727.3400](tel:202.727.3400), oag.dc.gov.

For Maryland Residents: You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888.743.0023, <https://www.marylandattorneygeneral.gov/>.



For New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These 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. For more information about the FCRA, please visit ftc.gov.

In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have the right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about obtaining a security freeze, go to <https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts>.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, [212-416-8433](tel:212-416-8433) or <https://ag.ny.gov/resources/individuals/credit-lending/identity-theft>; or 2) NYS Department of State's Division of Consumer Protection, [800-697-1220](tel:800-697-1220) or <https://dos.ny.gov/consumer-protection>.

For North Carolina Residents: You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, [1-877-566-7226](tel:1-877-566-7226), ncdoj.gov.

For Rhode Island Residents: You have the right to obtain a copy of the applicable police report, if any, relating to this incident. You may contact and obtain information from and/or report identity theft to your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street Providence, RI 02903; Phone: [401-274-4400](tel:401-274-4400); Website: www.riag.ri.gov