SECURITY BREACH NOTIFICATION SAMPLE

March 9, 2026

NOTICE OF DATA BREACH

Stockton Cardiology Medical Group ("Stockton Cardiology") is sending you this letter as part of our ongoing commitment to protecting the privacy and security of our patients' information. On January 17, 2026, we learned that certain information maintained by Stockton Cardiology may have been accessed by an unauthorized individual. We are providing this notice to inform you of the incident and in accordance with our obligations under the Health Insurance Portability and Accountability Act ("HIPAA") and applicable California privacy laws.

What Happened? On December 15, 2025, Stockton Cardiology identified suspicious emails that had been sent to several employees. Although the emails were promptly deleted as part of our initial remediation efforts, on January 17, 2026, we discovered that certain files maintained in the ordinary course of business and patient care may have been accessed and removed from our systems by the unauthorized individual. Immediately thereafter, we started our investigation to determine the scope of the breach and to restore the integrity of our system. On February 17, 2026, we learned that some of these files have since been publicly disclosed. The files involved may include personally identifiable information, protected health information, and certain company business records.

What information was involved? The information potentially involved in this incident may have included patient names, mailing addresses, email addresses, and billing records that may contain limited medical information associated with services provided.

What is Stockton Cardiology Medical Group doing to help? Stockton Cardiology Medical Group is offering affected individuals one (1) year of complimentary credit monitoring services through our partner vendor, Epiq. These services are intended to help monitor potential misuse of personal information.

What has Stockton Cardiology done since the breach to rectify the issue: We have taken a number of steps to investigate this breach and prevent any potential harm to you including retaining an independent security firm to assist in the investigation of the breach, making several improvements to the security configuration of our information systems, shutting down an older remote access service used by our staff, adding MFA (multi-factor authentication) to certain internal systems, resetting all passwords on all of our systems, and reviewing our policies for data retention, so that fewer "working" files are retained.

What can you do? You may take additional steps to protect yourself from harm, including:

- Registering a fraud alert with a credit bureau such as the ones listed here, and ordering your credit reports:
  - Experian: www.experian.com,
  - TransUnion: www.transunion.com
  - Equifax: www.equifax.com

SECURITY BREACH NOTIFICATION SAMPLE

- Monitor your bank and credit card statements

For More Information

We understand that this incident may cause concern or inconvenience, and we sincerely regret that it occurred. Stockton Cardiology Medical Group remains committed to providing high-quality care to our patients, including safeguarding the privacy and security of personal information. We have implemented policies and procedures designed to protect patient information and are continuing to review and enhance our security measures.

If you have any questions about this notice or need assistance, please contact Stockton Cardiology Medical Group at (209) 944-5750 Monday through Friday between 8 am-5 pm or email at: response@stocktoncardiology.com.

Sincerely,

Stockton Cardiology Medical Group

1B Credit Monitoring - Plus

SECURITY BREACH NOTIFICATION SAMPLE

How To Enroll:

1) Visit www.privacysolutionsid.com and click “Activate Account”
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score and Report[1]
1-Bureau VantageScore® 3.0 (annual) and 1-Bureau Credit Report.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users’ current or past addresses.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[2]
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[2]
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Plus, please call directly at 866.675.2006, Monday-Friday 9:00 a.m. to 5:30 p.m., ET