
Freeman Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103

Tel: 267.758.6009

www.fmglaw.com

December 28, 2022

**VIA U.S. REGULAR MAIL**
Consumer Protection Division
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

**RE: General Computer Resources, Inc. - Notice of Data Event**

Dear Sir or Madam:

We represent General Computer Resources, Inc. d/b/a GCR Professional Services. ("GCR"), which offers highly specialized engineering and IT staffing solutions in Burlington, Massachusetts. This submission is provided pursuant to the New Hampshire Data Breach Notification Statute of 2007, N.H. REV. STAT. § 359-C:19(V), which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of New Hampshire.

GCR was recently the victim of a computer malware event. Upon discovery, GCR performed an immediate scan of its network and began working with cyber incident specialists to investigate the event. GCR's investigation identified that portions of its network were accessed on separate occasions beginning on August 14, 2022, until September 3, 2022. GCR therefore performed a thorough review of the potentially accessed files on its network and confirmed on or about October 17, 2022, that certain historical files that could have been taken contained some personal information. Therefore, while GCR has no indication that any information has been misused, it is notifying potentially impacted individuals out of an abundance of caution. The types of personal information impacted include client names and Social Security numbers.

On or about December 23, 2022, GCR provided notice via U.S. regular mail of the incident to potentially affected individuals. A sample copy of the notice is attached as Exhibit "A" for your records. GCR provided this notification to a total of 31 individuals, one (1) of which is a resident of the State of New Hampshire.

As an added precaution, GCR's notice offered affected individuals twenty-four (24) months of credit monitoring and identity restoration services through IDX. The notice to the affected individuals also includes instructions on the use of this product as well as encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements and credit reports, immediately reporting errors or suspicious activity to the financial institution or issuing bank, and filing a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. GCR also included contact information for the major consumer reporting bureaus, state-specific regulators, and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so.

After discovering the incident, GCR reset passwords to all user accounts and implemented multi-factor authentication to prevent future unauthorized access. GCR partnered with computer forensics professionals to thoroughly investigate and reported the incident to federal law enforcement. In addition, GCR continues to review its policies and procedures for ways to enhance the existing protections it has in place for its organization. GCR is also notifying other state regulators as necessary.

I believe this provides you with all information necessary for your purposes and to comply with New Hampshire law. However, if anything further is needed, please contact me directly.

Respectfully,

**FREEMAN MATHIS & GARY, LLP**

Nicholas Jajko

# Exhibit “A”

TECHNICAL STAFFING
281 Cambridge Street, Suite 200
Burlington, MA 01803

To Enroll, Please Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [redacted]

December 23, 2022

[First Name] [Last Name]
[Address 1]
[City], [State] [Zip]

Dear [First Name] [Last Name]:

At General Computer Resources, Inc. d/b/a GCR Professional Services. ("GCR"), we take data security and privacy seriously. As part of that commitment, we are notifying you of a recent incident that may have affected your personal information, which was shared with GCR in the performance of our staffing services. Please read this letter carefully.

**What Happened**

GCR was recently the victim of a computer malware event. Upon discovery, we performed an immediate scan of our network and began working with cyber incident specialists to investigate the event. Our investigation identified that portions of our network were accessed on separate occasions beginning on August 14, 2022, until September 3, 2022. We therefore performed a thorough review of the potentially accessed files on our network and confirmed on or about October 17, 2022, that certain historical files that could have been taken contained some personal information. Therefore, while we have no indication that any information has been misused, we are notifying potentially impacted individuals **out of an abundance of caution.**

**What Information Was Involved**

You are receiving this letter because, based on our review, your name and Social Security number were present within a file accessible on an area of our network during the period of access. We reiterate, however, that we have no indication that any information about you has been misused but we are notifying potentially affected individuals out of an abundance of caution.

**What We Are Doing**

We take this event and the security of personal information entrusted to us very seriously. Upon discovery of the incident, we reset passwords to all user accounts and implemented multi-factor authentication to prevent future unauthorized access. We also reported the incident to federal law enforcement and continue to review our policies and procedures for ways to enhance the existing protections we have in place for our organization.

As an additional precautionary measure to help protect your information, we are offering a complimentary two (2) year membership of identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

**What You Can Do**

We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. We recommend you report errors or suspicious activity to your financial institution or issuing bank immediately. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation titled "Additional Steps to Help Protect Your Information" for contact information and resources you may take advantage of to protect against fraud or misuse, should you find it appropriate to do so.

You can enroll in the free IDX identity protection services by going **to https://app.idx.us/account-creation/protect** or calling **1-800-939-4170** and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is **June 1, 2023**.

**For More Information**

We are very sorry for any concern or inconvenience this incident has caused or may cause you, but please know that GCR continues to take data security and privacy seriously. If you have any other questions or concerns you may contact us at , Monday through Friday 9 am – 5 pm Eastern Standard Time.

Sincerely,

Deborah S. Finnerty
Chief Financial Officer

David S. Connor
President

## ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

**Review personal account statements and credit reports.** We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

| Equifax | Experian | TransUnion |
|---|---|---|
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 105069 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |

**Place Fraud Alerts.** A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

**Place a Security Freeze.** Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

**Obtain additional information** about the steps you can take to avoid identity theft from the following entities:

- **California Residents**: Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338) TTY: 1-866-653-4261. This notification was not delayed by law enforcement.


**1. Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you. **MyIDCare will include two-year enrollments into the below service components:**

**3. Review your credit reports**. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of 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.

**4. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring.

**SINGLE BUREAU CREDIT MONITORING** - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

**CYBERSCAN™** - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

**IDENTITY THEFT INSURANCE** - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

**FULLY-MANAGED IDENTITY RECOVERY** - ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.