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

November 21, 2023

K3699-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF DATA [INCIDENT/BREACH]

Dear Sample A. Sample:

TGI Direct, Inc. (“TGI” or "We") provides printing and mailing services to a variety of organizations nationwide, including [Extra1]. We are writing to make you aware of an incident that may impact the privacy of your personal information and/or protected health information (“PHI”).

What Happened? TGI uses a managed file transfer tool known as MOVEit. MOVEit manages data it collects and stores on behalf of our customers. Progress Software, the creators of MOVEit, recently shared that the tool had vulnerabilities unknown to them that may allow an unauthorized actor to access data inside the tool. An unauthorized actor exploited MOVEit’s vulnerabilities and accessed data without permission for companies, including TGI.

On May 28, 2023, TGI observed unusual activity within the MOVEit file transfer tool’s server. After securing our environment to limit any harm from that unusual activity, we started investigating what occurred. To help with that investigation, we brought in third-party cybersecurity specialists. The investigation determined that, for less than four hours on May 28, 2023, an unauthorized actor accessed or acquired some data stored in the server. TGI reviewed the data to understand what type of information it contained and to whom it related. On November 8, 2023, it was confirmed that some of your personal information was affected by the incident.

What Information Was Involved? Your [Extra2] were present in the impacted files. No Social Security numbers or financial information was involved. We have no evidence that any of your information was used for identity theft or fraud.

What We Are Doing. We take this incident and the obligation to safeguard the information in our care very seriously. After discovering the incident, we worked to confirm our system’s security and brought in specialists to help us investigate what happened. Progress Software created patches designed to fix MOVEit’s vulnerabilities, and we promptly applied the patches.

Although we have no evidence that your information has been misused, we are offering you 24 months of credit monitoring and identity restoration services through Experian. The services are at no cost to you, but you need to activate the services directly because we cannot do so for you legally. If you wish to activate these services, follow the instructions in the attached *Steps You Can Take to Help Protect Your Information*. We encourage you to enroll in these services.

What You Can Do. We encourage you to review your account statements and monitor your free credit reports over the next 12 to 24 months to look for identity theft and fraud, suspicious activity, or errors.

For More Information. If you have additional questions or concerns, please feel free to call our designated call center at **877-653-0349** toll-free Monday through Friday from 8 am – 10 pm Central; Saturday and Sunday from 10 am - 7 pm Central (excluding major U.S. holidays). You may also write to TGI Direct, Inc. at Attn: IT Department, 5365 Hill 23 Drive, Flint, Michigan 48507.

Sincerely,

Monica Weaver, CEO & President
TGI Direct, Inc.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for 24 months.

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 reach out to an Experian agent. If, after discussing your situation with an agent, 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).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** February 29, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- 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, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-653-0349 by February 29, 2024. Be prepared to provide engagement number **B109619** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and 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.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **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.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal /credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/ credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they

ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported promptly to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this incident. There are approximately 26 Rhode Island residents that may be impacted by this incident.

EXHIBIT B

[redacted]

Thank you for filing a breach notification via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your breach notification.

Please do not fax, email, or mail a copy of this breach notification to us as that may delay the processing of your breach notification.

If you have questions or would like to provide feedback about the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification process, or OCR's investigative process, please send us an email at OCRbreachreportingfeedback@hhs.gov.

* Breach Affecting: 500 or More Individuals
* Report Type: Initial Breach Report

* Are you a Business Associate filing on behalf of a Covered Entity? Yes

---

Business Associate

Completion of this section is required if the breach occurred at or by a Business Associate or if you are filing on behalf of a Covered Entity.

Name of Business Associate:	TGI Direct, Inc.
Street Address Line 1:	5365 Hill 23 Drive
Street Address Line 2:	
City:	Flint
State:	Michigan
ZIP:	48507

Business Associate Point of Contact Information

* First Name: Lynda * Last Name: Jensen
* Email: Ljensen@mullen.law

* Phone Number: (Include area code):

Contact Phones

Phone Number	Usage
(267) 930-2302	Work

Enter the contact information for all Covered Entities you are filing on behalf of.

Covered Entity 1

* Name of Covered Entity:	Blue Cross Blue Shield of Michigan
* Street Address Line 1:	600 E. Lafayette Blvd.
Street Address Line 2:	MC 1302
* City:	Detroit
* State:	Michigan

* ZIP: 48226

Business Associate Point of Contact Information

* First Name: Kelly * Last Name: Lange

* Email: klange@bcbsm.com

* Phone Number: (Include area code):

Contact Phones

Phone Number Usage
(313) 225-8554 Work

* Type of Covered Entity: Health Plan

Covered Entity 2

* Name of Covered Entity: NextBlue of North Dakota

* Street Address Line 1: 600 E. Lafayette Blvd.

Street Address Line 2: MC 1302

* City: Detroit

* State: Michigan

* ZIP: 48226

Business Associate Point of Contact Information

* First Name: Kelly * Last Name: Lange

* Email: klange@bcbsm.com

* Phone Number: (Include area code):

Contact Phones

Phone Number Usage
(313) 225-8554 Work

* Type of Covered Entity: Health Plan

Covered Entity 3

* Name of Covered Entity: Michigan Public School Employees Retirement System

* Street Address Line 1: 600 E. Lafayette Blvd.

Street Address Line 2: MC 1302

* City: Detroit

* State: Michigan

* ZIP: 48226

Business Associate Point of Contact Information

* First Name: Kelly * Last Name: Lange

* Email: klange@bcbsm.com

* Phone Number: (Include area code):

Contact Phones

Phone Number Usage
(313) 225-8554 Work

* Type of Covered Entity: Health Plan

Covered Entity 4

* Name of Covered Entity: State of Michigan

* Street Address Line 1:	600 E. Lafayette Blvd.
Street Address Line 2:	MC 1302
* City:	Detroit
* State:	Michigan
* ZIP:	48226

Business Associate Point of Contact Information

* First Name: Kelly * Last Name: Lange

* Email: klange@bcbsm.com

* Phone Number: (Include area code):

Contact Phones

Phone Number	Usage
(313) 225-8554	Work

* Type of Covered Entity: Health Plan

* Breach Start Date: 05/28/2023 * Breach End Date: 05/28/2023

* Discovery Start Date: 11/08/2023 * Discovery End Date: 11/08/2023

* Approximate Number of Individuals Affected by the Breach: 16113

---

* Type of Breach: Hacking/IT Incident

---

* Location of Breach: Network Server

---

* Type of Protected Health Information Involved in Breach:

Clinical
Demographic
Other

* Clinical

Diagnosis/Conditions
Medications
Other Treatment Information

* Demographic

Address/ZIP
Date of Birth
Name

* Type of Protected Health Information Involved in Breach (Other): Health insurance member identification number and insurance information.

---

* Brief Description of the Breach: TGI Direct, Inc. ("TGI") provides printing and mailing services to a variety of organizations, including health plans. On May 28, 2023, TGI observed unusual activity related to its MOVEit file transfer tool caused by a vulnerability discovered by the tool's maker, Progress Software. TGI took steps to ensure the security of its environment and launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the unauthorized

activity. On November 8, 2023, the investigation confirmed that personal information was present in the impacted files. TGI notified its clients and worked with them to identify address information for potentially impacted individuals in order to effect direct notice to them.

---

* Safeguards in Place Prior to Breach:	Privacy Rule Safeguards (Training, Policies and Procedures, etc.) Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.) Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.) Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

* Individual Notice Provided Start Date:	11/21/2023	Individual Notice Provided Projected/Expected End Date:	
Was Substitute Notice Required?	No		
Was Media Notice Required?	Yes		
* Select State(s) and/or Territories in which media notice was provided:	Michigan North Dakota		

---

* Actions Taken in Response to Breach:	Adopted encryption technologies Changed password/strengthened password requirements Implemented new technical safeguards Provided individuals with free credit monitoring Took steps to mitigate harm

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

* Name: Lynda Jensen Date: *11/21/2023*