Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

RECEIVED
OCT 02 2026
CONSUMER PROTECTION DIVISION
SEATTLE

RECEIVED
OCT 01 2026
AGO
General Services HLB

Clark Hill

Jason M. Schwent
T (312) 985-5939
F +13125177573
Email:jschwent@clarkhill.com

Clark Hill
1400 Wewatta Street, Suite 550
Denver, CO 80202
T (303) 943-9276

September 21, 2026

VIA PORTAL

Office of the Attorney General
1125 Washington St SE
Olympia, WA

Dear Attorney General Brown:

We represent the Friesen Group ("Friesen") as outside counsel with respect to a data security incident involving the potential exposure of certain personally identifiable information ("PII"). Friesen is a Covered Entity under the Health Insurance Portability and Accountability Act ("HIPAA") and has provided notice to impacted individuals and regulators in accordance with its requirements thereunder. Friesen takes the security of the patient information seriously and is committed to answering any questions you may have regarding this event to the best of its ability.

1. Nature of security incident.

On May 19, 2025, Friesen received a suspicious email that indicated data stored within Friesen's network may have been at risk. In response, Friesen took steps to secure its systems, initiated an investigation, and engaged a third-party forensic firm to assist. The investigation determined on July 15, 2025, that an unauthorized user gained access to Friesen's network for a limited period of time and may have accessed data. Friesen engaged a data review team to conduct a time-consuming and detailed reconstruction and analysis of the data and on July 16, 2026, the investigation determined that the unauthorized activity may have included access to some files containing the PII of residents of your state.

2. Number of residents affected.

Thirty-Eight (38) residents of Washington were notified of the incident. A letter was sent to potentially affected individuals on September 21, 2026. A copy of the template notification letter is enclosed.

3. Steps taken in response to the incident.

Upon discovering the incident, Friesen immediately implemented additional security measures to help secure its systems and prevent future unauthorized access. Additionally, Friesen is offering

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

identity theft protection services through TransUnion, a company specializing in fraud assistance and remediation services.

4. Contact Information

Friesen takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL



Jason Schwent
Member

cc: Wyatt Sugrue - wsugrue@clarkhill.com

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

The Friesen Group
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

FG FRIESEN GROUP

Jane A Smith Jr
123 Main St
Apt A
Sample, XX ABC12 DE34

September 21, 2026

Draft

NOTICE OF DATA SECURITY INCIDENT

Dear Jane Smith,

The Friesen Group ("Friesen"), is writing to let you know about a data security incident that may have involved some of your information. This letter contains information about steps you can take to protect your information and the resources we are making available to help you.

What Happened?

On May 19, 2025, we received a suspicious email that indicated data stored within Friesen's network may have been at risk. We immediately implemented our incident response protocols and engaged independent computer forensic experts to assist with an investigation to determine what occurred, and whether any sensitive information was impacted. The investigation determined on July 15, 2025, that an unauthorized user gained access to Friesen's network for a limited period of time and may have accessed data. We worked with a data review team to review the data and help determine who may have been impacted. On July 16, 2026, we determined your information was found within the potentially compromised data.

What Information Was Involved?

It appears that the potentially impacted information may include your name and the following: test data.

What We Are Doing:

We want to assure you that we are taking steps to minimize the risk of this happening in the future. Since the incident, we have worked to restore our systems, tightened access controls, and are evaluating additional technical safeguards to strengthen the security of our systems. In addition, we are offering identity theft protection services through Cyberscout, a TransUnion company, a company specializing in fraud assistance and remediation services, for twelve (12) months. With this protection, Cyberscout will help you resolve issues if your identity is compromised.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: **ABC123DEF456**. To receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

This letter also provides other precautionary measures you can take to protect your information. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information:

If you have questions, please call <<TFN>> Monday through Friday from 8:00 am to 8:00 pm Eastenr Standard Time. Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you.

Sincerely,

Friesen Group

Draft

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Recommended Steps to help Protect your Information

1. **Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. 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 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

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.

2. **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. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. **Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. **You can obtain additional information about** the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of [XX] Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Draft