<<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>
<<Country>>

NOTICE OF DATA BREACH

<<Date>>

Dear <<First Name>>,

We are writing to notify you that Fried, Frank, Harris, Shriver & Jacobson LLP ("Fried Frank") recently experienced a cybersecurity incident. As a large international law firm, we sometimes receive information from our clients and other third parties, including personal information, which we possess in connection with the services we provide. <<Variable Text (*Client Representation*)>> During these representations, Fried Frank obtained information about you that was affected in the cybersecurity incident. Please read this notice carefully, as it provides up-to-date information on what happened and what we have done in response.

What Happened?

On October 27, 2025, we learned that a single Fried Frank user account was compromised by an unauthorized third party, which was able to use the account to copy certain files from a Fried Frank shared network drive. Upon learning of the unauthorized access, we promptly contained the incident and blocked the unauthorized access. We conducted an investigation of the incident with the help of outside data security experts and reported the matter to law enforcement. Our investigation determined that the unauthorized third party obtained certain files, including files containing personal information, between October 23, 2025, and the early morning of October 28, 2025.

What Information Was Involved?

Our investigation has determined that some of your personal information was affected by this incident, including your <<Variable Text *(Data Elements)*>>.

Fried Frank believes, based on actions we have taken, the experience of our outside experts with the typical practices of this unauthorized third party and similar groups, and our ongoing monitoring, that the compromised data will not be distributed or used improperly. Further, we do

not have any indication that the unauthorized third party was targeting your personal information specifically.

What We Are Doing

Fried Frank takes this incident and our responsibility to protect personal information in our possession extremely seriously, and we have taken a range of steps to enhance our existing security controls.

As a precaution, we have engaged Equifax to provide two years of credit and identity monitoring services at no cost to you. These services include fraud consultation and identity theft restoration services.

To take advantage of these services:

1. You must activate your identity monitoring services by **<<Variable Text>>.** Your Activation Code will not work after this date.
2. Visit www.equifax.com/activate to activate your identity monitoring services.
3. Provide your Activation Code: **<<Variable Text>>.**

If you have any questions about this service or need assistance with enrollment, please see the "For More Information" section below.

What You Can Do

We strongly encourage you to take advantage of the credit and identity monitoring services we are providing to you free of charge. Remain vigilant and carefully review your online and financial accounts for any suspicious activity.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to the proper law enforcement authority.

If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file where relevant.

For More Information

Fried Frank has established a dedicated call center to answer questions. If you have any questions regarding this incident or the services available to you, please call 1-855-815-4018 Monday through Friday between the hours of 9am – 9pm EST.

You may also contact Fried Frank directly by email at [redacted]

Once again, we sincerely regret that this incident has occurred and have taken robust steps to address it.

Sincerely,

Karl Groskaufmanis
General Counsel
Fried, Frank, Harris, Shriver & Jacobson LLP

Additional Resources

- You can learn more about how to protect yourself against identity theft by visiting www.usa.gov/identity-theft, or by contacting the Federal Trade Commission (FTC) or your state's Attorney General to obtain information, including about how to avoid identity theft, place a fraud alert, and place a security freeze on your credit report. **Federal Trade Commission**, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft
- **Order Your Free Credit Report**: We encourage you to periodically obtain credit reports from the below credit agencies and have fraudulent transactions deleted. To obtain an annual free copy of your credit reports, visit **annualcreditreport.com**, call toll-free at 1-877-322-8228, or contact the major credit reporting agencies. Their contact information is as follows:

Equifax:	**Experian:**	**TransUnion:**
equifax.com	**experian.com**	**transunion.com**
equifax.com/freeze	**experian.com/freeze**	**transunion.com/freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-888-909-8872

- **Fraud Alert**: You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert puts creditors on notice that you might be a victim of fraud. Creditors will then follow certain procedures designed to protect you, including contacting you before they open new accounts or change your existing accounts. Placing a fraud alert can protect you but also may delay you when you seek to obtain credit.
- **Security Freeze**: You have the ability to place a security freeze on your credit report at no charge. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent but may delay your ability to obtain credit. To place a security freeze, you must contact each of the three credit bureaus listed above and may be required to provide your full name; SSN; date of birth; the addresses where you have lived over the past five years; proof of current address, such as a utility bill or telephone bill; a copy of a government issued identification card; and if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency.
- **Fraud or Identity Theft**: If you suspect theft, you should file a report to law enforcement, the FTC at www.identitytheft.gov, or the Attorney General in your state. If you are the victim of fraud or identity theft, you have the right to (1) notify the police and Attorney General of your state; and (2) file a police report relating to the incident and obtain a copy of the report.
- **Federal Fair Credit Reporting Act Rights**: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies (CRAs) use your information. The FTC has summarized consumers' FCRA rights as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to a credit score; you have the right to dispute incomplete or inaccurate information; CRAs must correct or delete inaccurate, incomplete, or unverifiable information; CRAs may not report outdated negative information; access to your file is limited; employers need your consent to receive your reports; you may limit "prescreened" credit and insurance offers based on your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580.
- **State-Specific Notices**. Residents of the following states should review the following information:
    - **For District of Columbia residents:** You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

- **For Maryland residents:** You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.

- **For New York residents:** You may consider placing a Security Freeze on your credit report. For more information on a Security Freeze or on how to avoid identity theft, contact the New York Department of State Division of Consumer Protection (http://www.dos.ny.gov/consumerprotection/; (800) 697-1220) or the New York State Office of the Attorney General (http://www.ag.ny.gov/home.html; (800) 771-7755).

- **For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226 to contact other nationwide consumer reporting agencies and to make freeze requests and obtain information on combating identity theft.

- **For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information about placing a security freeze, you can visit the Oregon Department of Justice Consumer Protection website at https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/.

- **For Vermont residents:** Helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General's website at http://www.ago.vermont.gov. If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802- 656-3183 (800-649-2424 toll free in Vermont only).

- **For Rhode Island residents:** For more information on how to prevent identity theft, you may contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903, (401) 274-4400, and https://riag.ri.gov/. You have the right to obtain a police report about this incident. You may be required to pay fees to a consumer reporting agency when placing a credit freeze on your credit file. <<Variable Text (Rhode Island individuals)>>.

<First Name> <Last Name>
Activation Code: **<Activation Code>**
Enrollment Deadline: **<Enrollment Deadline>**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

---

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

[4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **<Activation Code>** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.