David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, New York 11201
dmcmillan@constangy.com
Direct: 718.614.8371

April 3, 2024

**VIA EMAIL**

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
Email: breach.security@maine.gov

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Wysocki Family of Companies ("WFC") in connection with a recent data security incident described in greater detail below.

1. **Nature of the security incident.**

On November 21, 2023, WFC became aware of unusual activity on its network. In response, WFC took immediate steps to secure its digital environment and engaged a leading cybersecurity firm to conduct an investigation to determine whether any sensitive information may have been accessed or acquired during the incident. Based on that investigation, WFC learned that an unknown criminal actor gained unauthorized access to its network and acquired certain files, some of which contained individuals' personal information. WFC immediately undertook a comprehensive review of the impacted data to determine what may have been affected and the individuals involved. On December 8, 2023, WFC confirmed that personal information belonging to certain individuals may have been involved. WFC then took steps to notify those individuals as quickly as possible. Then on February 27, 2024, Wysocki determined that additional individuals were impacted during the incident, including a single (1) Maine resident.

Please note that we have no current evidence to suggest misuse or attempted misuse of any personal information in conjunction with this incident.

2. **Number of Maine residents affected.**

On April 3, 2023, Wysocki notified a single (1) Maine resident of this incident via first class U.S. mail. The information potentially impacted in connection with this incident includes name and Social Security number.

A sample copy of the notification letter is included with this correspondence.

**3. Steps taken relating to the Incident.**

As soon as WFC discovered this incident, WFC took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal information potentially impacted. In addition, WFC implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future.

WFC is notifying all potentially impacted individuals of this incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services.

WFC has established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-800-939-4170 from 8:00 A.M. to 10:00 P.M. CST on Monday through Friday. In addition, while WFC is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, WFC is also providing complimentary credit and identity protection services to notified individuals.

**4. Contact information.**

WFC remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

**/s/ David McMillan**

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter

Return to IDX:
4145 SW Watson Ave
Suite 400
Beaverton, OR 97005

<<First Name>> << Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

April 3, 2024

Subject: Notice of Data <<Variable Text 1 – Breach or Security Incident>>

Dear << First Name>> << Last Name>>:

We are writing to notify you of a cybersecurity incident at Wysocki Family of Companies ("WFC") that may have affected your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

**What Happened?** On November 21, 2023, WFC learned that it had experienced a potential data security event and, in response, took immediate steps to secure our network and engage cybersecurity experts to conduct an investigation to determine what happened. Based on that investigation, we learned that an unknown criminal actor acquired certain files from our network, some of which contained individuals' personal information. We then immediately undertook a comprehensive review of the impacted data to determine precisely what may have been affected and the individuals involved. That process concluded on February 27, 2024 and identified your information as potentially impacted, which is the reason for this notification.

**What Information Was Involved?** The information involved this incident may have included your name and your <Variable Text 2 – Data Elements>>. Please note that WFC has no evidence of any actual or suspected misuse of information involved in this incident.

**What We Are Doing:** As soon as we discovered this incident, we took steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, we have implemented several measures to enhance our security posture and reduce the risk of similar future incidents.

We are also offering you access to complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: <<12/24>> months of credit[1] and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

[1] To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

To enroll, please call 1-800-939-4170 or visit https://app.idx.us/account-creation/protect and provide the enrollment code at the top of this page. Please note you must enroll by July 3, 2024. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

**What You Can Do:** We encourage you to enroll in the credit protection services we are offering, which are at no cost to you. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

**For More Information:** If you have questions or need assistance, please contact 1-800-939-4170 Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Very truly yours,

**Bill Wysocki**

Wysocki Family of Companies
8550 Central Sands Road
Bancroft, WI 54921

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

**Fraud Alerts:** There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

**Credit or Security Freezes:** Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

**IRS Identity Protection PIN:** You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

**You also have certain rights under the Fair Credit Reporting Act (FCRA)**: These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

**Additional information:**

**District of Columbia**: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; oag@dc.gov.

**California**: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 1-800-952-5225; http://oag.ca.gov/.

**Maine:** Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 1-207-626-8800; https://www.maine.gov/ag/.

**Maryland**: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us.

**North Carolina**: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 1-877-5-NO-SCAM (Toll-free within North Carolina); 1-919-716-6000; www.ncdoj.gov.

**New York**: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 1-212-416-8433; https://ag.ny.gov/.

**Oregon:** Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us.

**Rhode Island**: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov.

**Texas**: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 1-800-621-0508; texasattorneygeneral.gov/consumer-protection/.

**Vermont**: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 1-802-828-3171; ago.info@vermont.gov.