Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Notice of Data Breach

Dear <<Full Name>>:

We are writing to notify you of a recent event that may have impacted your personal information. We are providing you with further information about the event, our response to it, and resources available to help protect your information, should you feel it appropriate to do so.

WHAT HAPPENED?

Between June 26, 2026 and July 6, 2026, an unauthorized third party gained access to Wikoff Color Corporation's ("Wikoff," "us," or "we") internal systems and acquired certain files. Upon becoming aware of the incident, we immediately commenced an investigation by hiring cybersecurity experts in an effort to secure our network, systems, and data, and to determine the nature and scope of the event. We further notified law enforcement.

We immediately undertook a review to determine the type of information contained in the acquired files. While that review is ongoing, we have identified your contact information to notify you of the security incident that involved your personal information.

WHAT INFORMATION WAS INVOLVED?

Based on our investigation to date, we understand that the unauthorized third party obtained files containing your full name in combination with your date of birth and Social Security number.

WHAT WE ARE DOING.

Upon becoming aware of the unauthorized access, we immediately acted to contain the unauthorized third party's access, commenced an investigation to determine the nature and scope of the access, and notified law enforcement. This included engaging forensic experts to secure our system and environment. As part of our ongoing commitment to information security, we are reviewing existing policies and procedures and enhancements to our technical security measures to reduce the likelihood of a similar event and to reinforce the integrity of our digital environment.

We also continue to review and enhance our safeguards as part of our ongoing commitment to protecting personal information. As an added precaution, we are providing credit monitoring at no cost to you for 24 months.

WHAT YOU CAN DO.

We encourage you to remain vigilant by reviewing your account statements and monitoring your credit reports for suspicious activity. If you identify any activity you do not recognize, you should promptly contact the financial institution or company with which the account is maintained. Please review the attachment to this letter, *Steps You Can Take to Further Protect Your Information*, for additional details on what you can do to better help protect yourself against possible misuse of your information, and how to activate your free credit monitoring services.

FOR MORE INFORMATION.

We understand the concern and inconvenience this may cause. For further information and assistance, please contact us at 888-616-9567 between 9:00 a.m. - 9:00 p.m. ET, Monday through Friday.

Sincerely,

Marc C. Lewis
President & CEO

Steps You Can Take to Further Protect Your Information

Enroll in Your Free Credit Monitoring Services

Review the attachment to this letter, *Epiq - Privacy Solutions ID*, for detailed instructions on how to enroll in your free credit monitoring services.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

Remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

How to Obtain and Monitor Your 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 www.annualcreditreport.com, calling toll-free 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 may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

	Equifax	Experian	TransUnion
Contact Information	(866) 349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	(888) 397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	(800) 888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19016

How to Place a Fraud Alert on Your Credit Report

You may also place a fraud alert 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. Please Note: No one is allowed to place a fraud alert on your credit report except you.

How to Place a Security (Credit) Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.

Obtain an Internal Revenue Service Identity Protection PIN (IP PIN)

You may obtain an IP PIN from the Internal Revenue Service – a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification 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. Information about the IP PIN program can be found here: irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

Additional Information

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.

- **All US Residents**: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, www.ftc.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.
- **California Residents**: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, 1-800-952-5225.
- **District of Columbia Residents:** Office of the Attorney General of the District of Columbia, 400 6th Street, NW, Washington, D.C. 20001, oag.dc.gov, 1-202-727-3400.
- **Iowa Residents**: Office of the Attorney General of Iowa, 1305 E. Walnut Street Des Moines, Iowa 50319, www.iowaattorneygeneral.gov, 888-777-4590
- **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, 1-502-696-5300.
- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023.
- **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**: Office of the Attorney General, The Capitol, Albany, NY 12224; www.ag.ny.gov/, 1-800-771-7755.
- **North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400.
- **Oregon Residents:** Office of the Attorney General, 1162 Court Street Northeast Salem, Oregon, 97301, www.doj.state.or.us/consumerprotection, 877-877-9392
- **Rhode Island Residents**: Office of the Attorney General, 160 South Main Street Providence, RI 02903, www.riag.ri.gov, 401-274-4400

<<Full Name>>
Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: 24 Months

Epiq - Privacy Solutions ID

1B Credit Monitoring - Plus

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score and Report[1]
1-Bureau VantageScore® 3.0 (annual) and 1-Bureau Credit Report.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[2]
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[2]
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Plus, please call directly at **866.675.2006,** Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.