<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>

Notice of Data Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing to tell you about a data security incident that may have exposed some of your personal information and to provide you with information about steps you can take to protect your identity. We take the protection and proper use of your information very seriously. We are contacting you at this time because we recently learned that this incident may have included personal information about you. For this reason, we are contacting you directly to explain the circumstances of the incident.

What Happened?
On February 1, 2024, Southwest Binding & Laminating ("Southwest") noticed unusual activity on its internal network from a Southwest domain account with administrator privileges. We immediately began investigating the incident, and after initial investigation, we determined we were the victim of a ransomware attack. We responded by immediately taking all servers offline. Additionally, on this same day, remediation efforts began, including efforts to restore critical business files and services. Among other things, as part of our investigation, mitigation, and remediation efforts, we engaged leading third-party cybersecurity forensic experts and other advisors to identify the scope of the incident and move quickly to mitigate the impact. As a result of our subsequent investigation, on February 22, 2024, we determined that some of the files the threat actor may have accessed in connection with the incident contained personal information of some of our current and former employees, and independent contractors, including independent contractors of our subsidiary Graphic Finishing Partners.

What Information Was Involved?
Based on our analysis of the incident to date, the personal information involved in this incident may have included your name, home address, government-issued identification number (for example, social security number). It also includes employee payroll information such as salary, employee status, payroll deduction amounts, direct deposit numbers, benefit status, and dependent information.

What We Are Doing.
While our investigation continues, we believe that we have stopped further unauthorized access of personal information on our servers. We have also engaged legal counsel to help us notify appropriate regulatory authorities. In addition, we are continuously monitoring our systems for any suspicious activity and have deployed additional resources to reinforce the security of our systems.

What You Can Do.
Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, 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.

For more information.

If you have questions for Southwest Binding & Laminating or Graphic Finishing Partners about this notice, please call 1-800-325-3628 ext 3014 Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time, and reference this letter. You may also write to Southwest Binding & Laminating at PO Box 150, Maryland Heights, MO, 63043. RE: Data Security Incident.

Protecting your information is important to us and we sincerely regret that this incident has occurred. We trust that this notice demonstrates our continued commitment to your security and satisfaction.

Sincerely,

Mark Mercer
President, Southwest Binding & Laminating
Subsidiary, Graphic Finishing Partners

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey and New Mexico residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

For New Mexico residents: Under the Fair Credit Reporting Act, you have the right to be told if information in the file the consumer reporting agency holds about you has been used against you, the right to know what is in your file, the right to ask for a credit score, and the right to dispute incomplete or inaccurate information. You may have additional rights depending on the circumstances or your status (i.e., Veteran).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

For Colorado, Illinois, Maryland, and Massachusetts residents: You can obtain information from the Federal Trade Commission and the three credit reporting agencies about fraud alerts, security freezes, and steps you can take to avoid identity theft.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338). The Federal Trade Commission can also provide you with information about fraud alerts and security freezes.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For 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/.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: We encourage you to report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.