20542

Skyline®

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

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

Re: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Skyline Displays, LLC ("Skyline") is contacting you to inform you of a data security incident involving some of your personal information. Skyline takes this matter very seriously and apologizes for any inconvenience caused. The intent of this letter is to share some information and resources for steps you can take to protect your personal information.

What Information Was Involved

Skyline began investigating the data security incident as soon as we became aware of it. Based on our extensive investigation, which included two outside forensics firms, we understand that in connection with the incident, the information stolen by the cybercriminal may have included your full name, address, phone number, Social Security number, credit card number, driver's license number, date of birth, passport number, and/or health information.

Credit Monitoring/Identity Theft Protection Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

- Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
- *You have until **September 3, 2021** to activate your identity monitoring services.*
- Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

What You Can Do

The security of personal information is a top priority for us. In order to help you reduce the risk that your personal information could be misused, we recommend that you take the following steps:

- Remain vigilant by reviewing your financial account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.
- Obtain a copy of your credit report from one of the three major credit reporting agencies (Equifax, Trans Union, and Experian). You should check these credit reports for any unauthorized transactions. By law, you have the right to obtain a free credit report from any of the three consumer reporting agencies each year.
- Consider having the credit reporting agencies place a fraud alert and security freeze on your credit report.
- For more information about protecting yourself from identity theft, the attached Exhibit A includes contact information for the FTC and the national credit reporting agencies, as well as other disclosures and recommendations.
- Do not respond to any suspicious emails or requests for personal or sensitive information.

Preventing Future Incidents

We remind you to remain vigilant with suspicious looking emails and to never open attachments within such emails. In addition, please note that Skyline will never ask you for your credentials, and you should never provide them if prompted to do so by an attachment in an email.

For More Information

We realize that you may have questions as to what this means and what you can do to protect yourself. For additional information, please call 1-855-537-2105, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some U.S. holidays.

We again sincerely apologize for any inconvenience caused by this incident. Protecting your information is important to us. We trust that we can continue to demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Elaine Prickel
Vice President of Human Resources

Exhibit A - Additional Information

FREE CREDIT REPORT

Under federal law, you are entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies by calling 1-877-322-8228, visiting www.annualcreditreport.com, 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.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should promptly notify your financial institution or company with which the account is maintained, and you should also call your local law enforcement agency and file a police report. You have a right to obtain a copy of the police report and you should obtain it, as many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at 1-877-ID-THEFT (1-877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations.

FRAUD ALERTS

We recommend that you remain vigilant by reviewing your account statements, monitoring the free credit report referenced above, and by placing a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax
(800) 525-6285
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 9532
Allen, TX 75013

TransUnion
(800) 680-7289
www.transunion.com
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

SECURITY FREEZES

You can request a "Security Freeze" on your credit file, free of charge, by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent.

The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale.

To place a Security Freeze, free of charge, on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(800) 685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com/freeze

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com/freeze

Information to Include:

- Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.)
- Your Social Security number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill bank or insurance statement or telephone bill
- If you have moved in the past five (5) years, give your previous addresses where you have lived for the past five (5) years.
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have up to three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have up to three (3) business days after receiving your request to remove the security freeze.

ADDITIONAL INFORMATION

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, or if you would like additional information regarding how to prevent identify theft, you should immediately contact the Federal Trade Commission and/or the Massachusetts Attorney General's office. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You can contact the **Federal Trade Commission** by visiting www.consumer.gov/idtheft or www.ftc.gov/idtheft, by calling the FTC at 1-877-382-4357, or by writing to the FTC at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You can 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

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit 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.