Troutman Pepper Hamilton Sanders LLP
5 Park Plaza, Suite 1400
Irvine, CA 92614-2545

troutman.com

troutman pepper

Ronald I. Raether, Jr.
ron.raether@troutman.com

June 8, 2021

VIA OVERNIGHT DELIVERY

Attorney General Thomas J. Miller
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Incident Notification

Dear Attorney General Miller:

This firm represents Progrexion ASG, Inc. ("Progrexion") which is located at 257 East 200 South, Salt Lake City, UT 84111. We are writing, pursuant to Iowa Code Ann. § 715C.2, to provide notice of an incident that occurred at Progrexion related to forty-six (46) Iowa residents. The incident did not involve the type of personal information that would constitute a breach as defined by Iowa Code Ann. § 715C.1. Nonetheless, Progrexion intends to provide notice to the Iowa residents and offer those residents Trans Union Trueldentity identity theft protection services.

The incident in question (the "Incident") was discovered on April 8, 2021, when Progrexion became aware of search patterns that suggested a malicious third-party was using Progrexion's public-facing platforms to request certain information to help individuals decide if Progrexion's services are needed. The malicious actor had apparently acquired names, email addresses, social security numbers, dates of birth, and other identifiers from a source other than Progrexion. The malicious third party then used the information it had in its possession to circumvent the controls Progrexion had in place to assure that information about a consumer went only to the consumer. As a result, the malicious third party could have had access to consumers' FICO scores, account numbers, the identity of financial institutions (*e.g.*, name of a bank) and/or limited tradeline transaction information (such as whether the consumer ever made a late payment). The malicious third party did not gain access to any passwords, social security numbers, or codes to access any consumer account that originated from Progrexion.

Upon discovering the Incident, Progrexion took the public-facing platforms offline. Progrexion is currently evaluating its platforms to determine if additional controls should be implemented to reduce the risk of a similar incident occurring in the future. In addition, Progrexion has notified the National Cybersecurity Communications and Integration Center (NCCIC) of the Incident. Progrexion will update you if any additional information is uncovered.

troutman pepper

We have attached a sample of the notification letter that Progrexion will send to the Iowa residents on or about June 16, 2021.

Should you have any questions or concerns about this matter, please do not hesitate to contact me.

Sincerely,

Ronald I. Raether, Jr.

Encl.

TEMPLATE

Company Letterhead

[DATE]

[CONTACT INFORMATION]

Re: An Important Message

Dear <<Name 1>>

On behalf of Progrexion ASG, Inc. ("Progrexion"), which is located at 257 East 200 South, Salt Lake City, UT 84111, we are writing to advise you of an incident ("Incident") that may involve unauthorized access to some of your personal information. Set forth below is important information concerning the Incident, along with some resources that may help you protect against the possibility of misuse of your information.

WHAT HAPPENED?
On April 8, 2021, Progrexion first discovered search patterns that indicated a malicious third-party was using Progrexion's public-facing platforms to request certain information to help individuals decide if Progrexion's assistance is required. While the information the malicious third party obtained did not include your Social Security number or any passwords or access codes to accounts that you maintain, it appears that the malicious third-party may have already possessed this or similar information about you from some source other than Progrexion. The malicious third party used this information to access Progrexion's public-facing platforms to possibly view your FICO score, account number, or institution identity (e.g., name of a bank) and limited details about that account (e.g., if any payments were late).

WHAT INFORMATION WAS INVOLVED?
The information that was potentially involved in the Incident may have included your FICO score, account numbers, or institution identity (e.g., name of a bank) and limited details about that account (e.g., if any payments were late, balances and the like). It is important to note that the third party did not access from Progrexion your Social Security number, or any passwords or access codes to accounts that you maintain.

WHAT ARE WE DOING?
Progrexion is committed to protecting the privacy of your information. Upon discovering the third party's actions, Progrexion took its public-facing platforms offline to prevent any additional fraudulent requests for information from being made. Progrexion is currently evaluating its platforms to determine if additional controls should be implemented to reduce the risk of a similar incident occurring in the future.. In addition, Progrexion has notified a law enforcement agency - the National Cybersecurity Communications and Integration Center (NCCIC) - to advise it of the Incident.

While the information potentially involved in the Incident did not include your Social Security number, or any passwords or access codes to accounts that you maintain, it appears that the malicious third party may have already possessed this or similar information obtained about you

from some source other than Progrexion. Accordingly, in an abundance of caution and to help you under the circumstances with any prior events unrelated to Progrexion, we have arranged and are paying for you to receive a twenty-four (24) month membership in Trans Union's TrueIdentity theft protection services. ***The details of how to obtain Trans Union's TrueIdentity theft protection services are attached to this letter.***

WHAT CAN YOU DO?

Outlined below are a number of ways that you can protect yourself.

1. **Sign Up for Credit Monitoring.** We encourage you to take advantage of the complimentary credit monitoring services we are providing. As noted above, a description of the credit monitoring services is provided in the attached material.

2. **Monitor Account Statements and Free Credit Reports.** You should remain vigilant for incidents of financial fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports.

3. **Contact the Federal Trade Commission, Law Enforcement, and Credit Bureaus.** To report identity theft incidents or learn about steps you can take to protect yourself from identity theft, you may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement. To learn more, you can go to the FTC's websites at www.IdentityTheft.gov and www.ftc.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

   You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance
Atlanta, GA 30374-0241	Allen, TX 75013	Division
www.equifax.com	www.experian.com	P.O. Box 2000
		Chester, PA 19016-2000
		www.transunion.com

4. **Obtain Free Copy of Credit Reports.** You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. TransUnion, Equifax and Experian are offering free weekly credit reports on www.AnnualCreditReport.com through April 20, 2022, as part of their efforts to support all Americans during the Covid-19 pandemic. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228.

5. **Additional Rights Under the FCRA.** You have rights pursuant to the FCRA, 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 FCRA, 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 violators. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

6. **Request Fraud Alerts and Security Freezes**. You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

   You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

   You must place your request for a freeze with each of the three national consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze	Experian Security Freeze	Trans Union Security Freeze
P.O. Box 105788	P.O. Box 9554	Fraud Victim Assistance Department
Atlanta, GA 30348	Allen, TX 75013	P.O. Box 160
(800) 349-9960	(888) 397-3742	Woodlyn, PA 19094
		(888) 909-8872

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. The addresses where you have lived over the prior two years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. 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.

If the request for a security freeze is made by toll-free number or secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the security freeze on your credit report. If the request is made by mail, the credit reporting agencies have three (3) business days after receiving the request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a mechanism to enable you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

To remove a security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. There is no fee to place or lift a security freeze.

7. **Additional Information for Certain States.** Please review the last page of this letter for additional information for certain states.

FOR MORE INFORMATION

Please do not hesitate to contact our support agents if you have any questions or concerns by calling [ ]. Our support agents are available Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding U.S. holidays.

Sincerely,

Encls.

TEMPLATE

ADDITIONAL INFORMATION FOR CERTAIN STATES

For residents of California: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For residents of the District of Columbia: For additional information about steps to take to avoid identity theft, you may contact the District of Columbia Attorney General at 441 4th Street, NW, Washington, DC 20001, (202) 727-3400, dc.oag@dc.gov. Additionally, you may also contact the Office of Consumer Protection at Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, consumer.protection@dc.gov.

For residents of Iowa: To report suspected incidents of identity theft, you may contact local law enforcement or the Iowa Attorney General's Office. You can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, http://www.iowaattorneygeneral.gov/.

For residents of Maryland: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission	Office of the Attorney General
Consumer Response Center	Consumer Protection Division
600 Pennsylvania Avenue, NW	200 St. Paul Place
Washington, DC 20580	Baltimore, MD 21202
(877) IDTHEFT (438-4338)	(888) 743-0023
http://www.ftc.gov/idtheft/	www.oag.state.md.us

For residents of Massachusetts: In addition to the above steps, under Massachusetts law, you have a right to obtain a police report with regard to the Incident. In addition, if you are the victim of identity theft, you have a right to file a police report and obtain a copy of it.

For residents of North Carolina: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission	North Carolina Department of Justice
Consumer Response Center	Attorney General Josh Stein
600 Pennsylvania Avenue, NW	9001 Mail Service Center
Washington, DC 20580	Raleigh, NC 27699-9001
(877) IDTHEFT (438-4338)	(919) 716-6400
www.consumer.gov/idtheft	http://www.ncdoj.com

For residents of New York: You may obtain security breach response information and identity theft and protection information from the FTC, the Department of State, Division of Consumer Protection, and the New York Attorney General's Office. These offices can be reached at:

TEMPLATE

Federal Trade Commission Consumer Response Center (877) IDTHEFT (438-4338) www.consumer.gov/idtheft	Department of State Division of Consumer Protection (800) 697-1220 https://www.dos.ny.gov/consumerprotection	Office of the Attorney General (800) 771-7755 https://ag.ny.gov/

For residents of Oregon: You may report suspected identity theft to law enforcement, including You may report suspected identity theft to law enforcement, including the Oregon Attorney General and the FTC. These offices can be reached at:

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 (877) IDTHEFT (438-4338) http://www.ftc.gov/idtheft/	Oregon Department of Justice 1162 Court St. NE Salem, Oregon 97301 (877) 877-9392 https://www.doj.state.or.us/

For residents of Rhode Island: You have the right to file or obtain a police report (should one be filed) and request a free security freeze, free of charge, as described above. Placing a security freeze may require that you provide certain personal information (*e.g.*, name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. You may also contact the Attorney General's office at: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400, http://www.riag.ri.gov/.

TEMPLATE

[TRANSUNION INFORMATION]