NOTICE OF DATA BREACH

Oldenburg Group Incorporated and its division, Visa Lighting (together, the "Company") is providing substitute notice of a data breach that may have involved some personal information of current and former employees, as well as their dependents and beneficiaries. The Company has communicated directly with individuals it believes may have been affected, but unfortunately does not have sufficient contact information to contact all individuals directly.

What Happened? The Company experienced a ransomware incident between May 4th and May 5th, where an attacker who appears to be associated with the Play ransomware group installed ransomware on the Company's primary servers and may have had access to personal information of current and former employees, as well as their dependents and beneficiaries, located on the servers. As soon as we became aware of the activity, we took steps to secure the servers and launched an investigation. The investigation has not yet been able to determine whether any of your personal information was viewed or exfiltrated by the attacker; however, we have not been able to rule out the possibility. Thus, in an abundance of caution, we searched the contents of the data residing on the impacted servers to identify individuals whose information may have been accessible by the attacker. Since we launched our investigation over the week of May 6th, we continued through May and June to rebuild our system and identify additional potentially impacted individuals, and we have determined that information including, but not limited to, name, email address, address, date of birth, Social Security number, driver's license number, financial account information, tax information, medical information, and health insurance information may have been accessible by the attacker. For some individuals, we do not have current address information to provide direct notice. Accordingly, we are posting this substitute notice on our website.

What Information Was Involved? The information accessed may have included personal information including, but not limited to name, email address, address, date of birth, Social Security number, driver's license number, financial account information, tax information, medical information, and health insurance information.

What We Are Doing? We value privacy and deeply regret that this incident occurred. The Company has retained third-party forensics, third-party IT services, and outside counsel to assist in the investigation and to determine what information may have been accessed. To further protect personal information, we are also taking steps to enhance our existing security protocols. In addition, we are offering credit monitoring and identity protection services to potentially impacted individuals through IDX Identity.

What You Can Do? While we are not currently aware of any actual misuse of information contained on the servers, we advise that any potentially impacted individuals remain vigilant by reviewing financial account statements and credit reports for any unauthorized activity. Please review the below for further information on steps you can take to protect your information and how to enroll in the credit monitoring and identity protection services we are making available to potentially impacted individuals.

For More Information: For further information and assistance, please call 1-888-970-0470 between Monday through Friday from 9 am – 9 pm Eastern Time or go to https://response.idx.us/oldenburg/.

Steps You Can Take to Further Protect Your Information

Obtain free credit monitoring and identity protection services provided by Oldenburg.

We have arranged with IDX Identity to provide potentially impacted with credit monitoring and identity protection services. To determine eligibility and to obtain assistance for enrolling, please contact IDX Identity at 1-888-970-0470.

IDX Identity enrollments will include enrollments in the following service components:

> **Credit Monitoring** – Monitoring of credit bureaus for changes to the customer's credit file such as new credit inquiries, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record. Credit monitoring only available for adults.
>
> **CyberScan®** – Dark web monitoring of underground websites, chat rooms and malware, 24/7, to identify trading or selling of members' personal information.
>
> **Identity Theft Insurance** – Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible. Coverage is subject to the terms, limits, and/or exclusions of the policy.
>
> **Fully-Managed Identity Recovery** – IDX's recovery service provides our members recovery and restoration for identity theft issues such as (but not limited to): Account Creation, Criminal ID Theft, Medical Fraud, Account Takeover, Rental Application, Tax Fraud, Benefit Fraud, Online Auction Fraud and Utility Creation. This service includes complete triage process for members who report suspicious activity, a personally assigned IDCare Specialist to fully manage recovery and restoration of each identity theft case and expert guidance provided for those with questions about identity theft and protective measures.

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 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. 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 state. 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 in order to correct your records.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or logging into the IDX website and filing a request for help.

Obtain and monitor your credit report.

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting bureaus once every 12 months by visiting http://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 can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three major credit reporting bureaus.

Consider placing a fraud alert on your credit report.

We recommend placing 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 bureaus identified below. The credit reporting bureau you contact must tell the other two, and all three will place an alert on their versions of your report. Additional information is available at http://www.annualcreditreport.com.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit reporting bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Put a security freeze on your credit file.

You also 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. Unlike a fraud alert, you must separately place a security freeze on your credit file with each credit reporting bureau. To place a security freeze, you may be required to provide the consumer reporting bureau 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.

After receiving your freeze request, each credit reporting bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. A freeze remains in place until you ask the credit reporting bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit reporting bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit reporting bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit reporting bureau. Otherwise, you need to make the request with all three credit reporting bureaus.

Should you wish to place a fraud alert or credit freeze, or to otherwise contact any of the three major credit reporting bureaus, please refer to their contact information below.

Equifax	**Experian**	**TransUnion**
1-888-378-4329	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com
Equifax Fraud Alert	**Experian Fraud Alert**	**TransUnion Fraud Alert**
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
Equifax Credit Freeze	**Experian Credit Freeze**	**TransUnion Credit Freeze**
P.O. Box 105788	P.O. Box 9554	P.O Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Take advantage of additional free resources on identity theft.

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit www.IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Obtain additional information.

You can obtain information from these sources about steps you can take to avoid identity theft as well as information about fraud alerts and security freezes.

- All US Residents: Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.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, Telephone: 1-800-952-5225.

- Iowa Residents: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, https://www.iowaattorneygeneral.gov, Telephone: 1-888-777-4590.

- Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 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/, Telephone: 1-888-743-0023.

- New York Residents: Office of the Attorney General of New York, The Capitol, Albany, NY 12224, https://ag.ny.gov, Telephone: 1-800-771-7755.

- North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.com, Telephone: 1-877-566-7226 or 1-919-716-6400.

- Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.