Edenred Pay
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057

Jane Sample
126 Main St
Apt A
Sample, XX ABC12 DE37

September x, 2026

Re: Notice of Data Breach

Dear Jane:

GlobalvCard LLC, dba Edenred Pay ("Edenred Pay"), part of Edenred Group, is writing to notify you of a data security incident that may have impacted information associated with you. We process information associated with you in connection with Edenred Pay's accounts payable and payments services. Please read this notice carefully, as it provides information about what happened and what we are doing in response.

What information was involved?
The information impacted appears to have included your name, mailing address, and Social Security number.

What are we doing?
Edenred Pay has taken steps to address the incident and further secure the relevant environment, including revoking compromised access credentials, securing impacted systems and applications, and implementing enhanced monitoring tools to assist with detection and response activities.

As an additional precaution, we are offering you two years of Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for two years from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: **ABC123DEF456**. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What can you do?
Edenred Pay is not aware of any malicious use of your information as a result of this incident. However, it is always advisable to remain vigilant against attempts at identity theft or fraud, including by reviewing your credit reports and account statements for suspicious activity. If you identify suspicious activity, you should contact the entity that maintains the account or information on your behalf.

Additional information about steps you can take to help protect your information is included in Attachment A.

For more information:
We have established a dedicated call center to answer questions. If you have questions regarding this incident or the identity monitoring services available to you, please call1-800-405-6108, Monday through Friday from 8:00 am to 8:00 pm ET, excluding major U.S. holidays.

Sincerely,

Scott Duval
General Counsel

CC: A. Hoffmann (via email)

Attachment A

Below are additional helpful tips you may want to consider to help protect your personal information.

Review Your Credit Reports and Account Statements; Report Incidents
It is always advisable to remain vigilant against attempts at identity theft or fraud, including by reviewing your free credit reports and account statements closely for signs of suspicious activity. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to the proper law enforcement authorities. 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 your local police or law enforcement, the Federal Trade Commission ("FTC"), and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. The FTC's contact details are provided below.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)
1-877-FTC-HELP (382-4357

Copy of 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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax	P.O. Box 740241 Atlanta, GA 30374	www.equifax.com www.equifax.com/personal/credit-report-services	800-685-1111
Experian	P.O. Box 2002 Allen, TX 75013	www.experian.com ww.experian.com/help	888-397-3742
TransUnion	P.O. Box 1000 Chester, PA 19016	www.transunion.com www.transunion.com/credit-help	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert
You have the option to place a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for one year. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. You may also obtain information about fraud alerts from the FTC.

Security Freeze
You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order 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 telephone bill. For more information about requesting a security freeze, you may contact the credit reporting agency at the contact information provided above. You may also obtain information about security freezes from the FTC.

Federal Fair Credit Reporting Act Rights
The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 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. Identity theft victims and active-duty military personnel have additional rights pursuant to the FCRA.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Additional Information
If you are the victim of fraud or identity theft, you have the right to file a police report. And you have the right to obtain a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.