

October 7, 2024

Via E-mail (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann., Com. Law § 14-3504, I am writing on behalf of MoneyGram Payment Systems, Inc. (“MoneyGram” or the “Company”) to inform you about the nature and circumstances of a recent cybersecurity issue.

On September 20, 2024, MoneyGram detected unauthorized activity involving certain of its corporate systems. Upon detecting the issue, MoneyGram took steps to contain and remediate it, including proactively taking certain systems offline, which temporarily impacted the availability of the Company’s services. The Company also activated its incident response plan and launched an investigation with the assistance of leading external cybersecurity experts. In addition, MoneyGram has been coordinating with law enforcement authorities. The Company’s systems are back online and MoneyGram has resumed normal business operations. The Company has no evidence that this issue involved ransomware.

Based on the Company’s investigation, which is ongoing, the Company determined that an unauthorized third party accessed and acquired personal information of certain consumers, including names, contact information (such as phone numbers, email and postal addresses), dates of birth, a limited number of Social Security numbers, copies of government-issued identification documents (such as driver’s licenses), other identification documents (such as utility bills), bank account numbers, MoneyGram Plus Rewards numbers, transaction information (such as dates and amounts of transactions) and, for a limited number of consumers, criminal investigation information (such as fraud). The types of impacted information varied by affected individual. At this time, the Company’s investigation is in its early stages and it is working diligently to review the relevant files to determine which individuals were affected by this issue and the types of data impacted. The Company does not know at this time whether personal information related to Maryland residents was compromised. The Company is posting notice on its website and issuing a press release

Office of the Attorney General

October 7, 2024

Page 2

regarding this issue. In addition, MoneyGram has arranged to provide U.S. consumers with identity protection and credit monitoring services for two years at no cost to them.

In addition, the Company determined that the unauthorized party accessed and acquired work-related personal information of Company employees, including employee names, work email addresses and telephone numbers, job titles and roles, work locations, company usernames, hashed company login passwords, and in a limited number of cases personal cell phone numbers. MoneyGram is requiring employees to reset their Company passwords. MoneyGram is notifying three employees who are Maryland residents of this issue.

Enclosed for your reference are copies of the notice materials MoneyGram is providing in connection with this issue.

Please do not hesitate to contact me if you have any questions.

Very truly yours,



Lisa J. Sotto

Enclosures

NOTICE OF DATA BREACH

October 7, 2024

To Our Consumers:

MoneyGram Payment Systems, Inc., recently learned of a cybersecurity issue affecting certain of our company's systems.

What Happened?

On September 27, 2024, we determined that an unauthorized third party accessed and acquired personal information of certain consumers between September 20 and 22, 2024. Our investigation into the issue is ongoing.

What Information Was Involved?

The impacted information included certain affected consumer names, contact information (such as phone numbers, email and postal addresses), dates of birth, a limited number of Social Security numbers, copies of government-issued identification documents (such as driver's licenses), other identification documents (such as utility bills), bank account numbers, MoneyGram Plus Rewards numbers, transaction information (such as dates and amounts of transactions) and, for a limited number of consumers, criminal investigation information (such as fraud). The types of impacted information varied by affected individual.

What We Are Doing

Upon detecting the issue, we took steps to contain and remediate it, including proactively taking certain systems offline, which temporarily impacted the availability of our services. We also launched an investigation with the assistance of leading external cybersecurity experts and have been coordinating with law enforcement. Our systems are back online and we have resumed normal business operations.

What You Can Do

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your free credit reports. If you are in the U.S. and would like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. U.S. residents can order a free credit report by visiting www.annualcreditreport.com or calling toll-free at 1-877-322-8228. The U.S. Reference Guide below provides recommendations by the U.S. Federal Trade Commission on the protection of personal information. We also recommend that you remain alert for unsolicited communications involving your personal information.

In addition, we have arranged to offer affected U.S. consumers identity protection and credit monitoring services for two years at no cost to you. The U.S. Reference Guide below provides information on activation of the services.

We regret any inconvenience this issue may have caused. If you have questions regarding this matter, please refer to the Frequently Asked Questions below or contact us at (833) 918-1122 toll-free, Monday through Friday 8 a.m. to 8 p.m. CT (excluding major U.S. holidays). Please be prepared to provide engagement number B132368 when calling.

U.S. Reference Guide

We encourage affected U.S. consumers to take the following steps:

Enroll in Complimentary Identity Protection and Credit Monitoring Services. We have arranged with Experian to help you protect your identity and your credit information for two years at no cost to you.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. Please be prepared to provide engagement number B132368 when calling. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity).

Please note that Identity Restoration is available for 24 months from the date of this letter with engagement number B132368. Identity Restoration does not require enrollment on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. We also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by January 31, 2025 (Your code will not work after this date)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/plus>
- Provide your activation code: **HREP574ART**

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*

- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance:**** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228 or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you are in the U.S. and detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For more information, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580 1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax
Equifax Information Services
LLC
P.O. Box 105069
Atlanta, GA 30348-5069
1-888-836-6351
www.equifax.com

Experian
Experian Inc.
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
TransUnion LLC
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your 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 to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology ("BIT")
28 Liberty Street
New York, NY 10005
(212) 416-8433
<https://ag.ny.gov/resources/individuals/consumer-issues/technology>

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your 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 on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)727-3400
www.oag.dc.gov

U.S. CONSUMERS: FREQUENTLY ASKED QUESTIONS

1. What happened?

MoneyGram Payment Systems, Inc., recently learned of a cybersecurity issue affecting certain of our company's systems. On September 27, 2024, we determined that an unauthorized third party accessed and acquired personal information of certain consumers between September 20 and 22, 2024. Our investigation into the issue is ongoing.

2. What did MoneyGram do when it discovered the issue?

Upon detecting the issue, we took steps to contain and remediate it, including proactively taking certain systems offline, which temporarily impacted the availability of our services. We also launched an investigation with the assistance of leading external cybersecurity experts and have been coordinating with law enforcement. Our systems are back online and we have resumed normal business operations.

3. What information has been compromised?

The impacted information included certain affected consumer names, contact information (such as phone numbers, email and postal addresses), dates of birth, a limited number of Social Security numbers, copies of government-issued identification documents (such as driver's licenses), other identification documents (such as utility bills), bank account numbers, MoneyGram Plus Rewards numbers, transaction information (such as dates and amounts of transactions) and, for a limited number of consumers, criminal investigation information (such as fraud). The types of impacted information varied by affected individual.

4. What should I do to help protect my information?

MoneyGram is offering affected consumers identity protection and credit monitoring services for two years at no cost to you. Details of the services are available in the Reference Guide. In addition, we recommend that you:

- Remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your free credit reports.
- Remain alert for unsolicited communications involving your personal information.
- Order a credit report. If you are in the U.S. and would like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. U.S. residents can order a free credit report by visiting www.annualcreditreport.com or calling toll-free at 1-877-322-8228.

5. What if I have additional questions?

If you have additional questions regarding this matter, please contact us at (833) 918-1122 toll-free, Monday through Friday 8 a.m. to 8 p.m. CT (excluding major U.S. holidays). Please be prepared to provide engagement number B132368 when calling.

NOTICE OF DATA BREACH

October [REDACTED], 2024

Dear Colleague:

We are writing to provide an update on the recent cybersecurity issue.

What Happened?

As you are aware, MoneyGram Payment Systems, Inc. recently identified a cybersecurity issue affecting certain of our systems. On September 22, 2024, we determined that an unauthorized third party accessed and acquired work-related personal information of our employees on September 20, 2024.

What Information Was Involved?

The types of impacted information varied by affected employee and included employee names, work email addresses and telephone numbers, job titles and roles, work locations, company usernames, hashed company login passwords, and in a limited number of cases, personal cell phone numbers.

What We Are Doing

Upon detecting the issue, we took steps to contain and remediate it, including proactively taking certain systems offline, which temporarily impacted the availability of our services. We also launched an investigation with the assistance of leading external cybersecurity experts and have been coordinating with law enforcement. Our systems are back online and we have resumed normal business operations. We take the security of our systems and data very seriously and have put in place additional safeguards to further protect our systems and data.

What You Can Do

If you have not already done so within the past month, please change your company login password as soon as possible. In addition, we recommend you change your password for any other online account on which you used a password that is the same as or similar to your company system password.

If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your free credit reports. We also recommend that you are cautious of any unsolicited communications involving your personal information. The Reference Guide below provides information on recommendations by the U.S. Federal Trade Commission on the protection of personal information. If you have any questions regarding this matter, please contact us at (833) 918-1122 toll-free, Monday through Friday 8 a.m. to 8 p.m. CT (excluding major U.S. holidays). Please be prepared to provide engagement number B132367 when calling.

Thank you for your continued hard work and dedication.

Sincerely,

[Insert name]

U.S. Reference Guide

We encourage you to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you are in the U.S. and detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For more information, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580 1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax
Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
1-800-525-6285
www.equifax.com

Experian
Experian Inc.
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
TransUnion LLC
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/resources/individuals/consumer-issues/technology>

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. You are encouraged to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
www.doj.state.or.us