September 15, 2022

VIA U.S. Mail
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

RE: Cash Express Security Incident

Dear Sir/Madam:

I am writing to notify you that Cash Express—a storefront lending company who does not operate locations in New Hampshire—determined on August 4, 2022, that it suffered a security incident resulting in the potential unauthorized access to a limited amount of personal information on two New Hampshire residents.

Cash Express was the target of a ransomware attack in late January 2022. On February 6, 2022, we became aware of unusual activity on our network. We promptly began working with cybersecurity experts to investigate and subsequently determined that an unauthorized third-party gained access to a portion of our computer system. Based on our investigation, we believe the unauthorized third-party had access from January 29, 2022, to February 6, 2022. Once we identified the data that may have been affected, we promptly engaged a data review firm to determine what information was in those files. We received those results on August 4, 2022. And we have been working since then to assess our notification obligations and identify correct addresses for the affected individuals.

Having reviewed the data, we have reason to believe that the threat actor potentially accessed the personal information of two New Hampshire residents. The threat actor may have accessed files containing some combination of: full names, dates of birth, contact information, government identification (such as a driver's license, Social Security, or passport number), financial information (such as a bank account and routing number), and limited medical information. At this time, we have no reason to believe the information was, or will be, misused.

We began notifying the potentially affected individuals on September 16, 2022, and we have attached templates of those notification letters. We are offering a free subscription to credit monitoring for any individual who had their Social Security number or driver's license number affected. In addition to providing notice, we have taken a variety of measures to bolster our security. For example, we modified security policies, implemented a universal password reset, adopted new restrictions on access to our data centers, and hired third-party experts to monitor our networks.

Please contact me if you have any questions or need any additional information regarding this incident.

Sincerely,

Garry McNabb
Chief Executive Officer
Cash Express, LLC
345 South Jefferson Ave., Suite 300
Cookeville, TN 38501

Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

<<FIRST_NAME>> <<MI>> <<LAST_NAME>>
<<ADDRESS1>>
<<CITY>>, <<state>> <<zip>>

September 15, 2022

NOTICE OF DATA BREACH

Dear <<First_Name>> <<Mi>> <<Last_Name>>:

We are writing to inform you about an incident that may have exposed your personal information to unauthorized persons.

WHAT HAPPENED

On February 6, 2022, we became aware of unusual activity on our network. We promptly began working with cybersecurity experts to investigate and subsequently determined that an unauthorized third party gained access to a portion of our computer system. Based on our investigation, we believe they had access from January 29, 2022, to February 6, 2022. Once we identified the data that may have been affected, we promptly engaged a data review firm to determine what information was in those files. We received those results on August 4, 2022. And we have been working since then to identify correct addresses for the affected individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the unauthorized third party accessed some of your personal information, which may include some combination of your full name, date of birth, contact information, government identification (such as your Social Security or driver's license number), and financial information (such as your bank account and routing number).

WHAT WE ARE DOING

We hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to protect your information.

WHAT YOU CAN DO

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: <<expiration date>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code: <<code>>**

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8056 by **<<expiration date>>** and provide them engagement number **<<engagement#>>**.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/DataBreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.

- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.

- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland
Attorney General
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York
Attorney General
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

North Carolina
Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC
Attorney General
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact us at (866) 252-4401, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Garry McNabb
Chief Executive Officer
Cash Express, LLC
345 South Jefferson Avenue
Suite 300
Cookeville, TN 38501

CASHEX-ADT-CM1

CASH EXPRESS

Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

<<FIRST_NAME>> <<MI>> <<LAST_NAME>>
<<ADDRESS1>>
<<CITY>>, <<state>> <<zip>>

September 15, 2022

NOTICE OF DATA BREACH

Dear <<First_Name>> <<Mi>> <<Last_Name>>:

We are writing to inform you about an incident that may have exposed your personal information to unauthorized persons.

WHAT HAPPENED

On February 6, 2022, we became aware of unusual activity on our network. We promptly began working with cybersecurity experts to investigate and subsequently determined that an unauthorized third party gained access to a portion of our computer system. Based on our investigation, we believe they had access from January 29, 2022, to February 6, 2022. Once we identified the data that may have been affected, we promptly engaged a data review firm to determine what information was in those files. We received those results on August 4, 2022. And we have been working since then to identify correct addresses for the affected individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the unauthorized third party accessed some of your personal information, which may include some combination of your full name, date of birth, contact information, government identification (such as your passport or military ID number), and financial information (such as your bank account and routing number). We have no reason to believe that your Social Security number or driver's license number was affected.

WHAT WE ARE DOING

We hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to protect your information.

WHAT YOU CAN DO

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/DataBreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.

- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.

- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland Attorney General
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York Attorney General
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC Attorney General
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact us at (866) 252-4401, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Garry McNabb
Chief Executive Officer
Cash Express, LLC
345 South Jefferson Avenue
Suite 300
Cookeville, TN 38501

CASHEX-ADT-NCMF