GT GreenbergTraurig

July 28, 2023

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

Re: Notification of Security Incident – Follow Up

Dear Attorney General Formella:

We are writing to provide an update to the notification we provided to your office on June 30, 2023 (the "June 30th Notification") on behalf of our client City National Bank of Florida ("CNBF"). On July 21, 2023, CNBF notified an additional 4 individuals who reside in New Hampshire regarding the MOVEit zero-day vulnerability data security incident referenced in the June 30th Notification. For the avoidance of doubt, this notification does not relate to a new data security incident. In total, CNBF has notified approximately 18 New Hampshire residents of the MOVEit data security incident referenced in the June 30th Notification and provided all individuals with of free credit monitoring and identity theft protection services.

CNBF remains dedicated to protecting the personal information in its control. We look forward to working with you to address any questions or concerns you may have regarding the incident.

Best Regards,

Jena Valdetero
Shareholder

JMV:

Schedule A
June 30th Notification

Held, Lisa L. (LSS-CHI-IP-Tech)

From: Held, Lisa L. (LSS-CHI-IP-Tech) on behalf of Valdetero, Jena (Shld-CHI-IP-Tech)
Sent: Friday, June 30, 2023 9:04 PM
To: attorneygeneral@doj.nh.gov
Cc: Held, Lisa L. (LSS-CHI-IP-Tech)
Subject: City National Bank of Florida - Notice of Data Security Incident
Attachments: CNBF_NH AG Notification Letter_063023.pdf

On behalf of attorney Jena Valdetero, attached please find notice of a data security incident made on behalf of City National Bank of Florida. Please contact our office with any questions.

Thank you,
Lisa Held

Lisa L. Held
Legal Support Specialist

Greenberg Traurig, LLP
77 West Wacker Drive | Suite 3100 | Chicago, IL 60601
T 312 364 1551 | C 815 953 4889
Lisa.Held@gtlaw.com | www.gtlaw.com

GT GreenbergTraurig

Jena M. Valdetero
Tel 312.456.1025
Fax 312.456.8435
Jena.valdetero@gtlaw.com

June 30, 2023

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

Re: Notification of Security Incident

Dear Attorney General Formella:

We are writing to inform you that our client, City National Bank of Florida ("CNBF") is notifying 14 individuals who reside in New Hampshire of a data security incident that may have impacted some of their personal information.

On May 31, 2023, Progress Software announced a previously unknown (Zero-Day) vulnerability affecting its MOVEit® Transfer application (SecureFT). City National Bank of Florida ("CNBF"), alongside many other organizations, utilizes this application for managed file transfers and other business purposes for a subset of its clients. CNBF immediately took the application offline and applied the available patches issued by Progress Software to fix the vulnerability. CNBF began investigating to determine if it was among one of the thousands of Progress Software customers affected. After a thorough investigation, on June 3, 2023, CNBF determined that certain information on the MOVEit Transfer application was removed on May 29-30th by an unauthorized party. CNBF has notified and is cooperating with federal law enforcement authorities and its federal regulators.

The information accessed could include some or all of the following:

Although CNBF has measures in place to protect customer bank accounts from misuse, it is offering to change account numbers upon request.

CNBF is mailing the attached notification letters in **Schedule A** to all potentially affected individuals beginning June 30, 2023. The three major Credit Reporting Agencies are also being notified.

CNBF is offering identity theft protection services through a data breach and recovery service, IDX, A ZeroFox Company. Services include of credit monitoring, a $1,000,000 identity

fraud loss reimbursement, fraud consultation, and identity theft restoration. Information regarding these services, as well as additional information to assist with enrollment, is included in the notification letter mailed to potentially affected individuals.

Please contact me for any additional information.

Best Regards,

Jena Valdetero
Shareholder

JMV:

Schedule A

Individual Notification Letters

City National Bank
Bci FINANCIAL GROUP

P.O. Box 1907
Suwanee, GA 30024

June 30, 2023

Dear ,

On May 31, 2023, Progress Software announced a previously unknown (Zero-Day) vulnerability affecting its MOVEit® Transfer application (SecureFT). City National Bank of Florida ("CNBF"), alongside many other organizations, utilizes this application for managed file transfers and other business purposes for a subset of our clients. We are unfortunately one of many organizations affected by this issue. This Zero Day vulnerability has impacted thousands of organizations, across all industries, and in many geographies around the world.

Please note, this has not, and will not, affect our ability to provide quality banking and financial services to our valued account holders and corporate clients. Now, as always, we are strictly focused on protecting our clients' deposits and transactions. Importantly, it is still safe to interact with our corporate systems, including online banking.

Our investigation determined that your personal information held at CNBF was affected. We are notifying you and providing tools you can use to help protect against possible identity theft or fraud, should you feel it is appropriate to do so.

WHAT HAPPENED: After Progress Software's announcement on May 31st, CNBF immediately began investigating to determine if it was among one of the thousands of Progress Software customers affected. We engaged third-party cybersecurity and forensics experts to assist us in our remediation and investigative efforts and notified law enforcement. On June 3rd, our investigation identified that certain information on the MOVEit Transfer application was removed on May 29-30th by an unauthorized party.

WHAT INFORMATION WAS INVOLVED: The information involved may have included your first

WHAT WE ARE DOING: Upon being notified of Progress Software's Zero-Day vulnerability, we immediately took the application offline and have applied the available patches issued by Progress Software to fix the vulnerability. We have implemented a number of additional security measures to increase our ability to monitor and detect any suspicious account activity. Although we are actively monitoring for suspicious account activity, if you are concerned and would like us to discuss options for changing your account number, please contact us at the number below.

To help relieve concerns and restore confidence following this incident, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

WHAT YOU CAN DO: We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling , going to , or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is September 30, 2023.

Affected individuals may consider freezing their credit to prevent loans, credit cards, and other services from being opened in their names without their permission. To initiate a credit freeze, contact each of the three national credit reporting agencies listed on the following page. Additional information is available at www.annualcreditreport.com. We also recommend you review your credit reports and account statements over the next and notify your financial institution of any unauthorized transactions or incidents of suspected identity theft. Refer to the enclosed "Important Additional Information" for other precautions you can take.

FOR MORE INFORMATION: If you have any questions about this incident, please go to , scan the QR image, or contact , Monday – Friday between 9:00 a.m. and 9:00 p.m. Eastern Time, excluding major U.S. holidays, or reach out to your relationship manager for more assistance.

Our clients are our utmost priority. We deeply regret the concern or inconvenience this incident may cause you and appreciate your patience and support.

Sincerely,

City National Bank of Florida

ENC: Important Additional Information

Important Additional Information

For residents of *Iowa*: *Y*ou are advised to report any suspected identity theft to law enforcement or to the Attorney General.
For residents of *Oregon*: *Y*ou are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.
For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. 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 see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were approximately 7 Rhode Island residents notified in this incident.

DC Attorney General	**Maryland Office of Attorney General**	**New York Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
400 6th Street NW Washington, DC 20001 1-202-727-3400 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 https://www.marylandattorneygeneral.gov/	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 https://ncdoj.gov/	150 South Main St Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

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

***Massachusetts and Rhode Island residents*:** You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies and have information relating to fraudulent transactions deleted. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send

you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

ransUnion Security Freeze
.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

City National Bank
Bci FINANCIAL GROUP

P.O. Box 1907
Suwanee, GA 30024

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/CityNational

[Name]
[ADDRESS]
[ADDRESS 2]
[CITY, STATE, ZIP]
[REF#: [REFERENCE#]

June 30, 2023

[Re: Notice of Data Breach]

Dear Parent or Guardian of [NAME]

On May 31, 2023, Progress Software announced a previously unknown (Zero-Day) vulnerability affecting its MOVEit® Transfer application (SecureFT). City National Bank of Florida ("CNBF"), alongside many other organizations, utilizes this application for managed file transfers and other business purposes for a subset of our clients. We are unfortunately one of many organizations affected by this issue. This Zero Day vulnerability has impacted thousands of organizations, across all industries, and in many geographies around the world.

Please note, this has not, and will not, affect our ability to provide quality banking and financial services to our valued account holders and corporate clients. Now, as always, we are strictly focused on protecting our clients' deposits and transactions. Importantly, it is still safe to interact with our corporate systems, including online banking.

Our investigation determined that your child's personal information held at CNBF was affected. We are notifying you and providing tools you can use to help protect your child against possible identity theft or fraud, should you feel it is appropriate to do so.

WHAT HAPPENED: After Progress Software's announcement on May 31st, CNBF immediately began investigating to determine if it was among one of the thousands of Progress Software customers affected. We engaged third-party cybersecurity and forensics experts to assist us in our remediation and investigative efforts and notified law enforcement. On June 3rd, our investigation identified that certain information on the MOVEit Transfer application was removed on May 29-30th by an unauthorized party.

WHAT INFORMATION WAS INVOLVED: The information involved may have included your child's first and last name, date of birth, bank account number, Social Security Number, email and mailing addresses.

WHAT WE ARE DOING: Upon being notified of Progress Software's Zero-Day vulnerability, we immediately took the application offline and have applied the available patches issued by Progress Software to fix the vulnerability. We have implemented a number of additional security measures to increase our ability to monitor and detect any suspicious account activity. Although we are actively monitoring for suspicious account activity, if you are concerned and would like us to discuss options for changing your child's account number, please contact us at the number below.

To help relieve concerns and restore confidence following this incident, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised.

WHAT YOU CAN DO: We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 888-775-8498, going to https://response.idx.us/CityNational, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is September 30, 2023.

Again, at this time, there is no evidence that your child's information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your child's personal information.

FOR MORE INFORMATION: If you have any questions about this incident, please go to https://response.idx.us/CityNational, scan the QR image, or contact 888-775-8498, Monday – Friday between 9:00 a.m. and 9:00 p.m. Eastern Time, excluding major U.S. holidays, or reach out to your relationship manager for more assistance.

Our clients are our utmost priority. We deeply regret the concern or inconvenience this incident may cause and appreciate your patience and support.

Sincerely,

City National Bank of Florida

ENC: Recommended Steps to Help Protect Your Child's Information

Recommended Steps to Help Protect Your Child's Information

For residents of *Iowa*: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.
For residents of *Oregon*: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.
For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. 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 see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were approximately 7 Rhode Island residents notified in this incident.

DC Attorney General	**Maryland Office of Attorney General**	**New York Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
400 6th Street NW	200 St. Paul Pl	120 Broadway, 3rd Fl	9001 Mail Service Ctr	150 South Main St
Washington, DC 20001	Baltimore, MD 21202	New York, NY 10271	Raleigh, NC 27699	Providence, RI 02903
1-202-727-3400	1-888-743-0023	1-800-771-7755	1-877-566-7226	1-401-274-4400
www.oag.dc.gov	https://www.marylandattorneygeneral.gov/	www.ag.ny.gov	https://ncdoj.gov/	www.riag.ri.gov

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

***Massachusetts and Rhode Island residents*:** You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies and have information relating to fraudulent transactions deleted. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

City National Bank
Bci FINANCIAL GROUP

P.O. Box 1907
Suwanee, GA 30024

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/CityNational

[Name]
[ADDRESS]
[ADDRESS 2]
[CITY, STATE, ZIP]
[REF#: [REFERENCE#]

June 30, 2023

[Re: Notice of Data Breach]

Dear Administrator/Executor of the Estate of [NAME],

On May 31, 2023, Progress Software announced a previously unknown (Zero-Day) vulnerability affecting its MOVEit® Transfer application (SecureFT). City National Bank of Florida ("CNBF"), alongside many other organizations, utilizes this application for managed file transfers and other business purposes for a subset of our clients. We are unfortunately one of many organizations affected by this issue. This Zero Day vulnerability has impacted thousands of organizations, across all industries, and in many geographies around the world.

Please note, this has not, and will not, affect our ability to provide quality banking and financial services to our valued account holders and corporate clients. Now, as always, we are strictly focused on protecting our clients' deposits and transactions. Importantly, it is still safe to interact with our corporate systems, including online banking.

Our investigation determined that your loved one's personal information held at CNBF was affected. We are notifying you and providing tools you can use to help protect your loved one against possible identity theft or fraud, should you feel it is appropriate to do so.

WHAT HAPPENED: After Progress Software's announcement on May 31st, CNBF immediately began investigating to determine if it was among one of the thousands of Progress Software customers affected. We engaged third-party cybersecurity and forensics experts to assist us in our remediation and investigative efforts and notified law enforcement. On June 3rd, our investigation identified that certain information on the MOVEit Transfer application was removed on May 29-30th by an unauthorized party.

WHAT INFORMATION WAS INVOLVED: The information involved may have included your loved one's first and last name, date of birth, bank account number, Social Security Number, email and mailing addresses.

WHAT WE ARE DOING: Upon being notified of Progress Software's Zero-Day vulnerability, we immediately took the application offline and have applied the available patches issued by Progress Software to fix the vulnerability. We have implemented a number of additional security measures to increase our ability to monitor and detect any suspicious account activity. Although we are actively monitoring for suspicious account activity, if you are concerned and would like us to discuss options for changing your loved one's account number, please contact us at the number below.

To help relieve concerns and restore confidence following this incident, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your loved one's identity is compromised. Please note that you may not be able to enroll if the Social Security Administration has notified the credit bureaus that your loved one is deceased.

WHAT YOU CAN DO: We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 888-775-8498, going to https://response.idx.us/CityNational, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is September 30, 2023.

Affected individuals may consider freezing their credit to prevent loans, credit cards, and other services from being opened in their names without their permission. To initiate a credit freeze, contact each of the three national credit reporting agencies listed on the following page. Additional information is available at www.annualcreditreport.com. We also recommend you review your loved one's credit reports and account statements over the next 12 to 24 months and notify your loved one's financial institution of any unauthorized transactions or incidents of suspected identity theft. Refer to the enclosed "Important Additional Information" for other precautions you can take.

FOR MORE INFORMATION: If you have any questions about this incident, please go to https://response.idx.us/CityNational, scan the QR image, or contact 888-775-8498, Monday – Friday between 9:00 a.m. and 9:00 p.m. Eastern Time, excluding major U.S. holidays, or reach out to your loved one's relationship manager for more assistance.

Our clients are our utmost priority. We deeply regret the concern or inconvenience this incident may cause you and appreciate your patience and support.

Sincerely,

City National Bank of Florida

ENC: Recommended Steps to Help Protect Your Loved One's Information

Recommended Steps to Help Protect Your Loved One's Information

For residents of *Iowa*: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.
For residents of *Oregon*: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.
For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. 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 see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were approximately 7 Rhode Island residents notified in this incident.

DC Attorney General	**Maryland Office of Attorney General**	**New York Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
400 6th Street NW Washington, DC 20001 1-202-727-3400 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 https://www.marylandattorneygeneral.gov/	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 https://ncdoj.gov/	150 South Main St Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

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

***Massachusetts and Rhode Island residents*:** You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies and have information relating to fraudulent transactions deleted. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send

you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800