Fwd: [External Sender] Data Security Breach Notice

1 message

---------- Forwarded message ---------
From: **Cyr, Gail** <Gail.Cyr@maine.gov>
Date: Thu, Apr 1, 2021 at 9:23 AM
Subject: [External Sender] Data Security Breach Notice
To: jonathan.olin@capitalone.com <jonathan.olin@capitalone.com>

Dear Mr. Olin:

We are in receipt of your updated data security breach notice dated February 26, 2021 regarding Capital One data breach. Would you please fill out and submit the security breach form online at https://appengine.egov.com/apps/me/maine/ag/reportingform. This form can also be found on the Maine Attorney General's website under Identity theft – then Privacy, identity theft and data security breaches – then on the right hand side will be "Electronic Maine Security Breach Reporting Form".

Also, would you please send me an email confirmation when you have submitted the form? Thank you very much!

Sincerely,

Gail Cyr

--

Jonathan Olin
Managing Vice President and Chief Counsel
Enterprise Regulatory Advisory • Legal

P.O. Box 30285
Salt Lake City, UT 84130-0285

February 26, 2021

Office of the Maine Attorney General
109 Sewall St
Augusta, ME 04330

Case No. DSE 191404

Dear Attorney General Aaron Frey:

We are writing to provide an update to the notification letter Capital One sent your Office on August 14, 2019, and the follow-up letter we sent your Office on September 11, 2019, about the data security incident that Capital One discovered on July 19, 2019, and which occurred on March 22 and 23, 2019. We are providing this update because we recently determined that the Social Security numbers of an additional twenty (20) Maine residents were in the data that the unauthorized individual accessed in 2019, bringing the total number of impacted Maine residents to one thousand two hundred and thirty-three (1,233). Please allow us to provide a brief reminder of what occurred in 2019, to explain what we learned recently, and to share the steps we are taking to notify and protect Maine customers.

As a reminder, the data security incident occurred when an individual outside of Capital One, without authorization, obtained certain types of personal information about our credit card customers and credit card applicants. The FBI arrested the unauthorized individual on July 29, 2019, and recovered the stolen data. Capital One understood at the time, and still understands today, that there is no evidence any of this data was misused or disseminated before the FBI quickly confiscated the individual's devices. The unauthorized individual is currently being prosecuted by the U.S. Department of Justice.

Immediately after the 2019 data security incident, Capital One conducted an analysis with the assistance of an external third-party expert to determine what information was accessed by the unauthorized individual. The data elements the unauthorized individual obtained included names, addresses, and email addresses relating to approximately 98 million consumers. Fortunately, for the vast majority of these consumers, the Social Security numbers and linked bank account numbers contained in the exfiltrated data set were tokenized and, therefore, unreadable by the unauthorized individual or any other third party.

As of August 29, 2019, Capital One determined that the untokenized bank account numbers and/or Social Security numbers of one thousand two hundred and thirteen (1,213) Maine

residents were obtained by the unauthorized individual. As of August 29, 2019, Capital One sent letters to each of those consumers, explaining what occurred. Capital One also offered each of the impacted Maine residents two years of credit monitoring services through the "myTrueIdentity" product offered by TransUnion. Further, Capital One provided the impacted Maine residents with information about how to protect themselves from fraud and identity theft.

Recently, Capital One re-examined the files that were impacted by the 2019 data security incident using new and more advanced tools. As part of this analysis, we determined that the untokenized Social Security numbers of an additional twenty (20) Maine residents were among the data to which the unauthorized individual gained access during the 2019 data security incident.

At this time, and after performing additional analysis, the Company does not expect that additional consumers will be notified beyond those previously noticed in 2019 and being provided notice now. We have attached examples of the customer notifications we are sending in connection with the personal information that was recently identified.

Even though Capital One understood in 2019, and still understands today, that there is no evidence any of this data was misused or disseminated before the FBI quickly confiscated the individual's devices, each notification letter contains an offer for two years of free credit monitoring and identity protection with TransUnion's myTrueIdentity credit monitoring service, as well as information about how consumers can protect themselves from fraud and identity theft. Each letter also contains information about a web page we established and have recently updated to explain what occurred. Finally, each letter lists the phone number for the dedicated customer service team trained to handle questions or concerns about this issue.

Capital One remains committed to maintaining high standards for customer service and customer data security, as well as transparency with our customers and regulators. Upon learning of the data security incident in 2019, Capital One immediately fixed the issue and promptly began working with federal law enforcement. We have invested heavily in cybersecurity and will continue to do so.

If you have any questions, comments or concerns, please contact Jonathan Olin, Managing Vice President and Chief Counsel, at (202) 596-5804, or Jonathan.Olin@capitalone.com.

Sincerely,

Jonathan Olin
Managing Vice President, Legal, Privacy and Financial Integrity

P.O. Box 30285
Salt Lake City, UT 84130-0285

February 26, 2021

[redacted]

Case No. DSE 191404

NOTICE OF DATA BREACH

Dear [redacted],

We are writing to notify you that your personal information was involved in a data security incident that we previously announced on July 29, 2019. The incident occurred on March 22 and 23, 2019, and was discovered by Capital One on July 19, 2019. On January 27, 2021, we discovered that your Social Security number and name were exposed in this previous data security incident. We know how unsettling this news can be—please allow us to share more information about what took place.

WHAT HAPPENED

In the 2019 data security incident, an individual outside of Capital One gained unauthorized access to, and obtained certain types of, personal information about our credit card customers and credit card applicants. The FBI arrested the unauthorized individual on July 29, 2019, and recovered the stolen data. We believe, based on the evidence, the stolen data was recovered before it was used or disseminated. The individual is currently being prosecuted by the U.S. Department of Justice.

Immediately after the 2019 data security incident, we conducted an analysis with the assistance of an external third-party expert to determine what information was accessed by the unauthorized individual. At that time, we did not identify you as one of the individuals whose Social Security number was part of the accessed data.

Recently, Capital One re-examined the files that were impacted by the 2019 data security incident using new and more advanced tools. As part of this analysis, we determined that your Social Security number was among the data to which the unauthorized individual gained access.

Even though we do not believe that the individual used your information for fraud or disseminated it, we are notifying you of this incident.

WHAT INFORMATION WAS INVOLVED

The personal information obtained by the individual included your name and Social Security number and also may have included your date of birth, contact information, and other customer and credit data.

WHAT ARE WE DOING

As a precaution, we're offering you two years of credit monitoring and identity protection with TransUnion's *my*TrueIdentity credit monitoring service at no cost to you. You can sign up for this service by using the enclosed code and instructions any time before June 06, 2021. Due to privacy laws, we cannot register you directly. This service will not auto-renew.

Additionally, we want to let you know that upon learning of the incident in 2019, Capital One immediately fixed the issue and promptly began working with federal law enforcement. We have invested heavily in cybersecurity and will continue to do so. We've also used what we learned from this incident to further strengthen our cyber defenses.

WHAT YOU CAN DO
In addition to your enrolling in the credit monitoring service, we've included a list of resources for protecting yourself against potential misuse of your personal information.

FOR MORE INFORMATION
We understand how important your privacy is and apologize for any worry or inconvenience this may cause you. We want you to know that we are here for you and welcome any questions. We've set up a dedicated website at www.capitalone.com/facts2019. We also invite you to call us at 1-844-388-8999. Our dedicated support team is standing by to answer your questions and care for your needs 24/7.

Sincerely,

Capital One

HOW TO ENROLL IN CREDIT MONITORING

As noted above, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service run by TransUnion® called *my*TrueIdentity for two years provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting agencies.

- To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code** [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file or to speak to a TransUnion representative if you believe you may be a victim of identity theft. TransUnion representatives are available Monday–Friday, 8 a.m.–8 p.m. ET.

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

- You can sign up for the online or offline credit monitoring service any time between now and **June 06, 2021**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, Experian or Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

- If you have questions about your online credit monitoring benefits, need help accessing your credit report or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday–Friday: 8 a.m.–9 p.m., Saturday–Sunday: 8 a.m.–5 p.m. ET.

- **Special note for minors affected by this incident:** The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

ADDITIONAL RESOURCES

It is always good practice to monitor your account statements for instances of fraud or identity theft and immediately report any suspected incidents to the relevant financial institution(s). Most fraudulent debits or charges can be refunded or removed from your account if the managing institution is alerted within a brief window. It is also good practice to monitor your credit reports, which are available to you free of charge.

Annual Credit Report. You may order a free annual credit report. To do so, please visit www.annualcreditreport.com or call 1-877-322-8228. You can also order your free annual credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed below. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or make certain changes to your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a free security freeze on your credit report. A security freeze will prevent a credit reporting agency from releasing information in your credit report without your express authorization. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency certain identifying information, 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.

Bureau Contact Information. You may contact the three nationwide credit reporting agencies about security freezes, fraud alerts and other related topics using the following:

Equifax:	**Experian:**	**TransUnion:**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

Federal Trade Commission and State Attorneys General Offices. 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 home state. You can also contact these agencies for information on how to prevent or avoid identity theft:

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

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
http://www.marylandattorneygeneral.gov/
1-888-743-0023 or 410-528-8662

North Carolina Office of the Attorney General
Mail Service Center 9001
Raleigh, NC 27699-9001
http://www.ncdoj.gov/
1-877-566-7226

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
https://oag.dc.gov/
1-202-727-3400

Reporting identity theft and obtaining a police report:

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how credit reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of credit 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; credit reporting agencies must correct or delete inaccurate, incomplete or unverifiable information; credit 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; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

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

P.O. Box 30285
Salt Lake City, UT 84130-0285

February 26, 2021

[redacted]

Case No. DSE 191404

NOTICE OF DATA BREACH

Dear [redacted],

We are writing to notify you that your personal information was involved in a data security incident that we previously announced on July 29, 2019. The incident occurred on March 22 and 23, 2019, and was discovered by Capital One on July 19, 2019. On January 27, 2021, we discovered that your Social Security number and name were exposed in this previous data security incident. We know how unsettling this news can be—please allow us to share more information about what took place.

WHAT HAPPENED

In the 2019 data security incident, an individual outside of Capital One gained unauthorized access to, and obtained certain types of, personal information about our credit card customers and credit card applicants. The FBI arrested the unauthorized individual on July 29, 2019, and recovered the stolen data. We believe, based on the evidence, the stolen data was recovered before it was used or disseminated. The individual is currently being prosecuted by the U.S. Department of Justice.

Immediately after the 2019 data security incident, we conducted an analysis with the assistance of an external third-party expert to determine what information was accessed by the unauthorized individual. At that time, we did not identify you as one of the individuals whose Social Security number was part of the accessed data.

Recently, Capital One re-examined the files that were impacted by the 2019 data security incident using new and more advanced tools. As part of this analysis, we determined that your Social Security number was among the data to which the unauthorized individual gained access.

Even though we do not believe that the individual used your information for fraud or disseminated it, we are notifying you of this incident.

WHAT INFORMATION WAS INVOLVED

The personal information obtained by the individual included your name and Social Security number and also may have included your date of birth, contact information, and other customer and credit data.

WHAT ARE WE DOING

As a precaution, we're offering you two years of credit monitoring and identity protection with TransUnion's *my*TrueIdentity credit monitoring service at no cost to you. You can sign up for this service by using the enclosed code and instructions any time before June 06, 2021. Due to privacy laws, we cannot register you directly. This service will not auto-renew.

Additionally, we want to let you know that upon learning of the incident in 2019, Capital One immediately fixed the issue and promptly began working with federal law enforcement. We have invested heavily in cybersecurity and will continue to do so. We've also used what we learned from this incident to further strengthen our cyber defenses.

WHAT YOU CAN DO
In addition to your enrolling in the credit monitoring service, we've included a list of resources for protecting yourself against potential misuse of your personal information.

FOR MORE INFORMATION
We understand how important your privacy is and apologize for any worry or inconvenience this may cause you. We want you to know that we are here for you and welcome any questions. We've set up a dedicated website at www.capitalone.com/facts2019. We also invite you to call us at 1-844-388-8999. Our dedicated support team is standing by to answer your questions and care for your needs 24/7.

Sincerely,

Capital One

HOW TO ENROLL IN CREDIT MONITORING

As noted above, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service run by TransUnion® called *my*TrueIdentity for two years provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting agencies.

- To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code** [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file or to speak to a TransUnion representative if you believe you may be a victim of identity theft. TransUnion representatives are available Monday–Friday, 8 a.m.–8 p.m. ET.

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

- You can sign up for the online or offline credit monitoring service any time between now and **June 06, 2021**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, Experian or Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

- If you have questions about your online credit monitoring benefits, need help accessing your credit report or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday–Friday: 8 a.m.–9 p.m., Saturday–Sunday: 8 a.m.–5 p.m. ET.

- **Special note for minors affected by this incident:** The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

ADDITIONAL RESOURCES

It is always good practice to monitor your account statements for instances of fraud or identity theft and immediately report any suspected incidents to the relevant financial institution(s). Most fraudulent debits or charges can be refunded or removed from your account if the managing institution is alerted within a brief window. It is also good practice to monitor your credit reports, which are available to you free of charge.

Annual Credit Report. You may order a free annual credit report. To do so, please visit www.annualcreditreport.com or call 1-877-322-8228. You can also order your free annual credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed below. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or make certain changes to your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a free security freeze on your credit report. A security freeze will prevent a credit reporting agency from releasing information in your credit report without your express authorization. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency certain identifying information, 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.

Bureau Contact Information. You may contact the three nationwide credit reporting agencies about security freezes, fraud alerts and other related topics using the following:

Equifax:	**Experian:**	**TransUnion:**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

Federal Trade Commission and State Attorneys General Offices. 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 home state. You can also contact these agencies for information on how to prevent or avoid identity theft:

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

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
http://www.marylandattorneygeneral.gov/
1-888-743-0023 or 410-528-8662

North Carolina Office of the Attorney General
Mail Service Center 9001
Raleigh, NC 27699-9001
http://www.ncdoj.gov/
1-877-566-7226

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
https://oag.dc.gov/
1-202-727-3400

Reporting identity theft and obtaining a police report:

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how credit reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of credit 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; credit reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; credit 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; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

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

P.O. Box 30285
Salt Lake City, UT 84130-0285

26 de febrero de 2021

Número de Caso DSE 191404

AVISO DE ACCESO NO AUTORIZADO A INFORMACIÓN CONFIDENCIAL

Estimado(a) [redacted]:

Le escribimos para notificarle que su información personal estuvo involucrada en un incidente de seguridad de datos que anunciamos anteriormente el 29 de julio del 2019. El incidente ocurrió el 22 y el 23 de marzo del 2019 y fue descubierto por Capital One el 19 de julio del 2019. El 27 de enero del 2021 descubrimos que su número de Seguro Social y su nombre fueron expuestos en ese incidente de seguridad de datos anterior. Sabemos que esta noticia puede ser inquietante. Por favor permítanos compartir más información sobre lo que sucedió.

QUÉ SUCEDIÓ

En el incidente de seguridad de datos del 2019, una persona ajena a Capital One tuvo acceso no autorizado y obtuvo ciertos tipos de datos personales sobre nuestros clientes de tarjeta de crédito y solicitantes de tarjetas de crédito. El FBI arrestó a la persona no autorizada el 29 de julio del 2019 y recuperó la información robada. Creemos, con base en las pruebas existentes, que la información robada se recuperó antes de que fuera utilizada o difundida. La persona está siendo procesada actualmente por el Departamento de Justicia de los Estados Unidos.

Inmediatamente después del incidente de seguridad de datos del 2019, llevamos a cabo un análisis con la ayuda de un experto externo independiente para determinar a qué información tuvo acceso la persona no autorizada. En ese momento, no le identificamos a usted como una de las personas cuyo número de Seguro Social fue parte de la información a la que se obtuvo acceso.

Recientemente, Capital One reexaminó los archivos que se vieron afectados por el incidente de seguridad de datos del 2019 usando herramientas nuevas y más avanzadas. Como parte de este análisis, determinamos que su número de Seguro Social estaba entre los datos a los que tuvo acceso la persona no autorizada.

Aunque no creemos que la persona usó su información para cometer fraude ni que la haya divulgado, le estamos notificando sobre este incidente.

QUÉ INFORMACIÓN FUE AFECTADA

La información personal obtenida por la persona incluye su nombre y su número de Seguro Social y también puede que haya incluido su fecha de nacimiento, información de contacto y otros datos del cliente y de crédito.

QUÉ ESTAMOS HACIENDO
Como medida de precaución, le estamos ofreciendo dos años de monitoreo de crédito y protección de identidad con el servicio de monitoreo de crédito *my*TrueIdentity de TransUnion, sin costo alguno para usted. Usted puede inscribirse en este servicio usando el código y las instrucciones que se incluyen aquí en cualquier momento antes del 06 de junio del 2021. Debido a las leyes de privacidad, nosotros no podemos inscribirle directamente. Este servicio no se renovará automáticamente.

Además, queremos informarle que tan pronto nos enteramos del incidente en el 2019, Capital One solucionó el problema de inmediato y rápidamente comenzó a trabajar con las autoridades federales. Hemos invertido mucho en la seguridad cibernética y continuaremos haciéndolo. También hemos usado lo que aprendimos de este incidente para fortalecer aún más nuestras defensas cibernéticas.

LO QUE USTED PUEDE HACER
Además de inscribirse en el servicio de monitoreo de crédito, hemos incluido una lista de recursos que pueden ayudarle a protegerse contra el posible uso indebido de su información personal.

PARA MÁS INFORMACIÓN
Sabemos lo importante que es su privacidad, y lamentamos cualquier inquietud o inconveniente que esto pueda ocasionarle. Queremos dejarle saber que estamos aquí para ayudarle y puede hacernos cualquier pregunta. Hemos establecido y dedicado un sitio web en www.capitalone.com/digital/facts2019/es/. También puede llamarnos al 1-844-388-8999. Nuestro equipo de apoyo está disponible para responder a sus preguntas y atender sus necesidades, 24 horas al día, 7 días a la semana.

Atentamente,

Capital One

CÓMO INSCRIBIRSE EN MONITOREO DE CRÉDITO

Como se mencionó anteriormente, hemos acordado que usted se inscriba por dos años, sin costo alguno para usted, en un servicio de monitoreo de crédito de tres agencias por internet administrado por Transunion® llamado *my*TrueIdentity, ofrecido por TransUnion Interactive, una subsidiaria de TransUnion, que es una de las tres agencias de información de crédito a nivel nacional.

- Para inscribirse en este servicio, visite el sitio web de *my*TrueIdentity en www.mytrueidentity.com (servicio disponible en inglés únicamente) **y en el espacio que se indica como "Enter Activation Code" (Ingresar Código de Activación), ingrese el siguiente Código de Activación único de 12 letras** [redacted] y siga los tres pasos para recibir su servicio de monitoreo de crédito por internet en unos minutos.

- Si no tiene acceso a internet y desea inscribirse en un servicio de monitoreo de crédito similar en formato impreso y sin conexión, a través del servicio de Correo postal de EE.UU., por favor llame gratis a la línea de ayuda de TransUnion Fraud Response Services al **1-855-288-5422** (servicios en inglés únicamente). Cuando se le pida, ingrese el siguiente código de acceso telefónico de 6 dígitos [redacted] y siga los pasos para inscribirse en el servicio de monitoreo de crédito sin conexión a internet, agregue una alerta de fraude inicial a su expediente de crédito o hable con un representante de TransUnion si cree que es posible que sea una víctima de robo de identidad. Los representantes de TransUnion están disponibles de lunes a viernes, de 8 a.m. a 8 p.m., Hora del Este.

- Una vez que se inscriba, podrá obtener dos años de acceso ilimitado a su reporte de crédito y a su puntaje de crédito suministrados por TransUnion. El servicio de monitoreo de crédito diario de las tres agencias le notificará si hay cambios críticos en sus expedientes de crédito en TransUnion®, Experian® y Equifax®, incluidas alertas de fraude, verificaciones nuevas, cuentas nuevas, registros públicos nuevos, pagos atrasados, cambio de dirección y más. El servicio también incluye acceso a un programa de restablecimiento de identidad que le ofrece asistencia en el caso de que su identidad esté en riesgo para ayudarle a reestablecer su identidad y hasta $1,000,000 en seguro por robo de identidad sin deducible. (La Póliza puede estar sujeta a ciertas limitaciones y exclusiones).

- Puede inscribirse en el servicio de monitoreo de crédito, ya sea o no por internet, en cualquier momento desde ahora hasta el **06 de junio del 2021**. Debido a las leyes de privacidad, nosotros no podemos inscribirle directamente. Por favor tenga presente que es posible que los servicios de monitoreo de crédito no estén disponibles para individuos que no tengan un expediente de crédito con TransUnion, Experian o Equifax, o una dirección en Estados Unidos (o sus territorios) y un número de Seguro Social válido. La inscripción en este servicio no afectará su puntaje de crédito.

- Si tiene preguntas sobre sus beneficios de monitoreo de crédito por internet, si necesita ayuda para obtener acceso a su reporte de crédito o para aprobar la verificación de identidad, por favor comuníquese con el Equipo de Servicio al Cliente de *my*TrueIdentity gratis al 1-844-787-4607 en el siguiente horario: de lunes a viernes, de 8 am a 9 pm, y sábados a domingos, de 8 am a 5 pm, Hora del Este.

- **Nota especial para menores de edad afectados por este tipo de incidente:**
  Puede que los servicios arriba mencionados no estén disponibles para menores afectados. Como alternativa, los padres/tutores legales pueden investigar para ver si su niño(a) podría ser víctima de robo de identidad usando el formulario seguro por internet de TransUnion en www.transunion.com/childidentitytheft para enviar su información y para que TransUnion pueda verificar en su base de datos si hay un expediente de crédito con el número de Seguro Social de su niño(a). Después de que TransUnion complete la búsqueda, le responderán a la dirección de correo electrónico que usted proporcione. Si ellos localizan un archivo a nombre de su niño(a), le pedirán información adicional para poder proceder con medidas para proteger a su niño(a) contra impactos relacionados con esta actividad de fraude.

RECURSOS ADICIONALES

Siempre es una buena práctica monitorear sus estados de cuenta para detectar casos de fraude o robo de identidad y reportar de inmediato cualquier incidente sospechoso a las instituciones financieras pertinentes. La mayoría de los débitos o los cargos fraudulentos se pueden reembolsar o eliminar de su cuenta si la institución administradora recibe una alerta prontamente. También es una buena práctica monitorear sus reportes de crédito, los cuales están disponibles sin costo alguno.

Reporte de Crédito Anual. Usted puede pedir un reporte de crédito anual gratis. Para pedirlo, por favor visite www.annualcreditreport.com o llame al 1-877-322-8228 (servicios disponibles en inglés únicamente). Usted también puede pedir su reporte de crédito anual gratis enviando por correo postal un “Formulario de Solicitud del Reporte de Crédito Anual” (Annual Credit Report Request Form) ya completado (disponible en el sitio web de la Comisión Federal de Comercio de los EE.UU. (“FTC”) en www.consumer.ftc.gov/articles/0155-free-credit-reports) a: Annual Credit Report Request Service, Box 105281, Atlanta, GA 30348-5281.

Para los residentes de Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico y Vermont: Usted puede obtener una o más copias adicionales de su reporte de crédito, sin costo alguno (dependiendo del estado). Debe comunicarse directamente con cada una de las agencias de reporte de crédito para obtener los reportes adicionales.

Alerta de Fraude. Usted puede colocar una alerta de fraude en su registro comunicándose con una de las tres agencias de crédito nacionales mencionadas a continuación. Una alerta de fraude les indica a los acreedores que sigan ciertos procedimientos, incluso comunicarse con usted antes de abrir cuentas nuevas o hacer ciertos cambios en sus cuentas existentes. Por esa razón, colocar una alerta de fraude le puede proteger, pero también le puede demorar cuando necesite obtener crédito.

Congelamiento por Seguridad. Usted puede colocar un congelamiento por seguridad sin costo en su reporte de crédito. Un congelamiento por seguridad evitará que una agencia de información de crédito divulgue información de su reporte de crédito sin su autorización expresa. Un congelamiento por seguridad está diseñado para evitar que posibles acreedores tengan acceso a su reporte de crédito sin su consentimiento. Como resultado, un congelamiento por seguridad puede interferir con su capacidad para obtener crédito o demorarlo. Usted debe colocar un congelamiento por seguridad en su expediente de crédito con cada una de las agencias de información de crédito por separado. Para colocar un congelamiento por seguridad, puede ser que se le requiera presentar a la agencia de información de crédito cierta información de identificación, lo que incluye su nombre completo; número de Seguro Social; fecha de nacimiento; direcciones actual y pasada; una copia de su tarjeta de identidad emitida por el estado; y una copia reciente de su factura de servicio público, estado de cuenta bancario o factura del seguro.

Información de Contacto de las Agencias. Usted se puede comunicar con las tres agencias de información de crédito a nivel nacional y obtener información sobre congelamientos por seguridad, alertas de fraude y otros temas relacionados, a través de:

Equifax:	**Experian**:	**TransUnion:**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

Oficinas de la Comisión Federal de Comercio y de los Fiscales Generales de los Estados (Federal Trade Commission and State Attorneys General Offices). Si usted cree que ha sido víctima de robo de identidad o tiene motivos para creer que su información personal fue utilizada de manera indebida, debe comunicarse inmediatamente con la Comisión Federal de Comercio (FTC) y/o la oficina del Fiscal General en su estado de residencia. Usted también puede comunicarse con estas agencias para informarse sobre cómo prevenir o evitar el robo de identidad.

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

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
http://www.marylandattorneygeneral.gov/
1-888-743-0023 o 410-528-8662

North Carolina Office of the Attorney General
Mail Service Center 9001
Raleigh, NC 27699-9001
http://www.ncdoj.gov/
1-877-566-7226

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
https://oag.dc.gov/
1-202-727-3400

Para reportar robo de identidad y obtener un reporte policial.

Para los residentes de Iowa: Se le aconseja reportar cualquier sospecha de robo de identidad a las autoridades o al Fiscal General de Iowa.	**Para los residentes de Massachusetts:** Usted tiene el derecho de obtener un reporte policial con respecto a este incidente. Si usted es víctima de robo de identidad, también tiene el derecho de presentar un reporte ante la policía y obtener una copia del mismo.	**Para los residentes de Oregón:** Le aconsejamos reportar toda sospecha de fraude de identidad a las autoridades, incluyendo la Comisión Federal de Comercio (Federal Trade Commission) y el Fiscal General de Oregón.	**Para los residentes de Rhode Island:** Usted tiene el derecho de presentar u obtener un reporte policial con respecto a este incidente.

Ley Federal del Derecho a Informes de Crédito Justos: La Ley de Informes de Crédito Justos (FCRA) es una ley federal que regula cómo las agencias de reporte del consumidor usan su información. Promueve la exactitud, justicia, y privacidad de la información del consumidor en los expedientes de las agencias de información de crédito. Como consumidor, usted tiene ciertos derechos bajo la Ley de Informes de Crédito Justos (FCRA), los cuales la Comisión Federal de Comercio (FTC) ha resumido según se detalla a continuación: se le debe informar si la información en su expediente ha sido usada en su contra; usted tiene el derecho a saber qué está en su expediente; usted tiene el derecho a solicitar su puntaje de crédito; usted tiene el derecho a impugnar información incompleta o incorrecta; las agencias de información de crédito deben corregir o borrar información incorrecta, incompleta, o no verificable; las agencias de información de crédito del consumidor no pueden reportar información negativa desactualizada; el acceso a su expediente es limitado; usted debe dar su consentimiento para que los reportes sean proporcionados a empleadores; usted puede limitar las ofertas “preseleccionadas” de crédito y de seguro que usted recibe basado en la información en su reporte de crédito; usted puede reclamar a los infractores por daños. Las víctimas de robo de identidad y el personal militar en servicio activo tienen derechos adicionales.

Para más información sobre estos derechos, puede visitar www.ftc.gov/credit o escribir a: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

P.O. Box 30285
Salt Lake City, UT 84130-0285

February 26, 2021

[redacted]

Case No. DSE 191404

NOTICE OF DATA BREACH

Dear [redacted],

We are writing to provide you with an update to the letter we sent you on August 15, 2019, about a data security incident that we discovered on July 19, 2019, and which occurred on March 22 and 23, 2019. On January 27, 2021, in connection with a re-examination of the files obtained by the unauthorized individual, we discovered that your Social Security number was exposed during the 2019 data security incident. We know how unsettling this news can be—please allow us to share more information about what took place.

WHAT HAPPENED

As explained in the letter we sent you on August 15, 2019, the 2019 data security incident involved an individual outside of Capital One who gained unauthorized access to, and obtained certain types of, personal information about our credit card customers and credit card applicants. The FBI arrested the unauthorized individual on July 29, 2019, and recovered the stolen data. We believe, based on the evidence, the stolen data was recovered before it was used or disseminated. The individual is currently being prosecuted by the U.S. Department of Justice.

Immediately after the 2019 data security incident, we conducted an analysis with the assistance of an external third-party expert to determine what information was accessed by the unauthorized individual. At that time, we did not identify you as one of the individuals whose Social Security number was part of the accessed data. However, we did conclude that the unauthorized individual accessed other personal information belonging to you. We shared information about that in the letter we sent to you on August 15, 2019.

Recently, Capital One re-examined the files that were impacted by the 2019 data security incident using new and more advanced tools. As part of this analysis, we determined that your Social Security number was among the data to which the unauthorized individual gained access.

Even though we do not believe that the individual used your information for fraud or disseminated it, we are notifying you of this incident.

WHAT INFORMATION WAS INVOLVED

The personal information the individual may have obtained included the information listed in our letter dated August 15, 2019, as well as your Social Security number.

WHAT ARE WE DOING

As a precaution, we're providing a new offer for two years of credit monitoring and identity protection with TransUnion's *my*TrueIdentity credit monitoring service at no cost to you. You can sign up for this service by using the enclosed code and instructions any time before June 06, 2021. Due to privacy laws, we cannot register you directly. This service will not auto-renew.

Additionally, we want to let you know that upon learning of the incident in 2019, Capital One immediately fixed the issue and promptly began working with federal law enforcement. We have invested heavily in cybersecurity and will continue to do so. We've also used what we learned from this incident to further strengthen our cyber defenses.

WHAT YOU CAN DO
In addition to you enrolling in the credit monitoring service, we've again included a list of resources for protecting yourself against potential misuse of your personal information.

FOR MORE INFORMATION
We understand how important your privacy is and apologize for any worry or inconvenience this may cause you. We want you to know that we are here for you and welcome any questions. We've set up a dedicated website at www.capitalone.com/facts2019. We also invite you to call us at 1-844-388-8999. Our dedicated support team is standing by to answer your questions and care for your needs 24/7.

Sincerely,

Capital One

HOW TO ENROLL IN CREDIT MONITORING

As noted above, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service run by TransUnion® called *my*TrueIdentity for two years provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting agencies.

- To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code** [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft. TransUnion representatives are available Monday–Friday, 8 a.m.–8 p.m. ET.

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,® Experian® and Equifax,® including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

- You can sign up for the online or offline credit monitoring service any time between now and **June 06, 2021**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, Experian or Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

- If you have questions about your online credit monitoring benefits, need help accessing your credit report or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday–Friday: 8 a.m.–9 p.m., Saturday–Sunday: 8 a.m.–5 p.m. ET.

- **Special note for minors affected by this incident:** The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

ADDITIONAL RESOURCES

It is always good practice to monitor your account statements for instances of fraud or identity theft and immediately report any suspected incidents to the relevant financial institution(s). Most fraudulent debits or charges can be refunded or removed from your account if the managing institution is alerted within a brief window. It is also good practice to monitor your credit reports, which are available to you free of charge.

Annual Credit Report. You may order a free annual credit report. To do so, please visit www.annualcreditreport.com or call 1-877-322-8228. You can also order your free annual credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed below. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or make certain changes to your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a free security freeze on your credit report. A security freeze will prevent a credit reporting agency from releasing information in your credit report without your express authorization. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency certain identifying information, 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.

Bureau Contact Information. You may contact the three nationwide credit reporting agencies about security freezes, fraud alerts and other related topics using the following:

Equifax:	**Experian**:	**TransUnion:**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

Federal Trade Commission and State Attorneys General Offices. 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 home state. You can also contact these agencies for information on how to prevent or avoid identity theft:

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

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
http://www.marylandattorneygeneral.gov/
1-888-743-0023 or 410-528-8662

North Carolina Office of the Attorney General
Mail Service Center 9001
Raleigh, NC 27699-9001
http://www.ncdoj.gov/
1-877-566-7226

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
https://oag.dc.gov/
1-202-727-3400

Reporting identity theft and obtaining a police report:

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.	**For Massachusetts residents:** You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.	**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.	**For Rhode Island residents:** You have the right to file or obtain a police report regarding this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how credit reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of credit 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; credit reporting agencies must correct or delete inaccurate, incomplete or unverifiable information; credit 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; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

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