



Federal Employee Program.

1310 G Street, N.W.  
Ste. 900  
Washington, D.C. 20005  
www.fepblue.org

March 30, 2020

[IndividualFirstName] [Individual LastName]

[Address1]

[Address2]

[City], [State] [Zip Code]

### **Notice of Data Breach**

Dear [IndividualFirstName]:

I am writing to let you know of an incident affecting the MyBlue<sup>®</sup> Member Portal and involving your information.<sup>1</sup>

#### **What happened?**

We recently learned that a software code change made to the MyBlue Member Portal inadvertently altered Blue Cross and Blue Shield Federal Employee Program (FEP) member users' access for a short period of time. The change was made as part of a good faith effort to improve FEP members' secure access to their information, due to changes being made to a third-party web browser's security requirement. Through this code change, we have learned that your personal and health information may have been accessible to other MyBlue Portal members between the evening of February 4, 2020 and the morning of February 5, 2020. When we learned of this issue on the morning of February 5, 2020, we promptly terminated all member access to the MyBlue Member Portal to investigate and remediate the issue. As a result of the investigation, by February 25, 2020, we were able to determine that your personal information may have been accessible to another FEP member who had logged into the MyBlue Portal with their own MyBlue credentials during the brief incident window. However, to date, we are not aware of any misuse of the information that was potentially accessible because of this incident.

---

<sup>1</sup> This notice is being sent by the Blue Cross Blue Shield Association on behalf of the independent Blue Cross and/or Blue Shield Companies that administer the Federal Employee Program<sup>®</sup> ("FEP<sup>®</sup>") in their individual locations. The specific name of the Blue Cross and/or Blue Shield Plan to which your FEP membership is assigned is listed on the back of your insurance ID card.

### **What information may have been involved?**

Although we were able to conclude that your personal and health information was accessible to another FEP member during the incident window, we are unable to determine what specific information, if any, was accessed. This is because the information that may have been accessible through the MyBlue Member Portal to another FEP member varied by member. However, the information may have included (1) information to identify and contact you (such as first, middle, and last name, address, phone number(s), Social Security number, email address, group and member ID numbers, and date of birth); (2) information related to medical and/or claims histories (such as medical providers, dates of service, diagnoses, treatment information, test results and medical records); and (3) information regarding prescriptions, including drug name, number, prescriber name and pharmacy name. The incident did not involve potential access to your full financial account, or credit or debit card numbers.

### **What we are doing.**

As soon as we discovered the incident, we promptly took down the MyBlue Member Portal and launched an investigation. We resolved the issue and then restored the MyBlue Member Portal services. Since resolution, we have not been notified of the issue recurring, although we continue to monitor the Portal for any related issues.

While we are unaware of any misuse of your information as a result of this incident, including your credit or financial information, in an abundance of caution we have nonetheless arranged to offer you credit monitoring and identity restoration services for a period of two years, free of charge through Experian. You have until June 30, 2020 to activate these services, and instructions on how to activate these services are included in the attachments to this letter.

### **What you can do.**

As mentioned above, we are not aware of any misuse of your information to date as a result of this matter. The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to remain vigilant in monitoring your account statements, bills, notices, and insurance transactions for incidents of any unusual or unauthorized activity, and to promptly report such incidents to your health care provider or your local Blue Cross and/or Blue Shield Plan. Additionally, as a proactive step, we encourage you to review your personal information contained on the MyBlue Member Portal.

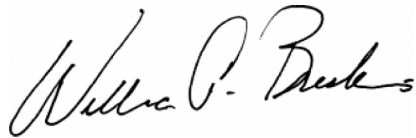
Blue Cross Blue Shield Association is an association of independent Blue Cross and Blue Shield companies.

**For More Information.**

If you have any questions about this matter or would like additional information, please call the FEP National Information Center toll free at 1-800-411-BLUE (2583) (callers may press #1, then press #0 to speak to a live agent). This call center is open Monday through Friday, 8 a.m. until 8 p.m. Eastern Standard Time, excluding weekends and holidays. We apologize for any concern this event may cause you and we greatly appreciate your understanding.

We regret that this incident occurred. We take the privacy of your personal information with the utmost seriousness and have implemented steps to prevent this in the future.

Sincerely,

A handwritten signature in black ink that reads "William A. Breskin". The signature is written in a cursive style with a large initial "W" and "B".

William A. Breskin  
Senior Vice President, Government Programs

Blue Cross Blue Shield Association is an association of independent Blue Cross and Blue Shield companies.

## Reference Guide

### **Review Your Account Statements**

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for health insurance statements, to your health plan.

### **Provide any updated personal information to your health care provider**

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

### **Order Your Free Credit Report**

To order your free annual credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus (Equifax, Experian and TransUnion) provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

### **How to Enroll in Experian's® IdentityWorks<sup>SM</sup>**

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks<sup>SM</sup>.<sup>1</sup> This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

---

<sup>1</sup> Experian®, IdentityWorks<sup>SM</sup>, and Experian IdentityWorks ExtendCARE™ are trademarks owned by Experian Information Solutions, Inc., an independent global information services company offering consumer credit reporting and a suite of identity detection and identity theft resolution services. Learn more at [www.experianplc.com](http://www.experianplc.com).

- Ensure that you **enroll by: June 30, 2020** (Your code will not work after this date)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: [INSERT INDIVIDUAL CODE FROM PIN CODE EXCEL FILE]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **866.579.5479** by **June 30, 2020**. Be prepared to provide engagement number **DB18701** as proof of eligibility for the identity restoration services by Experian.

#### **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **866.579.5479** (be prepared to provide engagement number **DB18701** as proof of eligibility for the identity restoration services by Experian). If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

### **Contact the U.S. Federal Trade Commission**

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

### **Place a Fraud Alert on Your Credit File**

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

### **Security Freezes**

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for

the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Freeze	Security	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	<a href="http://www.equifax.com">www.equifax.com</a>
Experian Freeze	Security	P.O. Box 9554 Allen, TX 75013	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion		P.O. Box 160 Woodlyn, PA 19094	888-909-8872	<a href="http://www.transunion.com">www.transunion.com</a>

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

#### **For Residents of Iowa**

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

Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)

#### **For Residents of Maryland**

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division  
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, <http://www.marylandattorneygeneral.gov/>

#### **For Residents of New Mexico**

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity;
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

#### **For Residents of North Carolina**

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division  
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov)

#### **For Residents of Oregon**

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392,  
[www.doj.state.or.us](http://www.doj.state.or.us)





Federal Employee Program.

1310 G Street, N.W.  
Ste. 900  
Washington, D.C. 20005  
www.fepblue.org

March 30, 2020

[IndividualFirstName] [Individual LastName]

[Address1]

[Address2]

[City], [State] [Zip Code]

### **Notice of Data Breach**

Dear [IndividualFirstName]:

I am writing to let you know of an incident affecting the MyBlue® Member Portal and involving your information.<sup>1</sup>

#### **What happened?**

We recently learned that a software code change made to the MyBlue Member Portal inadvertently altered Blue Cross and Blue Shield Federal Employee Program (FEP) member users' access for a short period of time. The change was made as part of a good faith effort to improve FEP members' secure access to their information, due to changes being made to a third-party web browser's security requirement. Through this code change, we have learned that your personal and health information may have been accessible to other MyBlue Portal members between the evening of February 4, 2020 and the morning of February 5, 2020. When we learned of this issue on the morning of February 5, 2020, we promptly terminated all member access to the MyBlue Member Portal to investigate and remediate the issue. As a result of the investigation, by February 25, 2020, we were able to determine that your personal information may have been accessible to another FEP member who had logged into the MyBlue Portal with their own MyBlue credentials during the brief incident window. However, to date, we are not aware of any misuse of the information that was potentially accessible because of this incident.

---

<sup>1</sup> This notice is being sent by the Blue Cross Blue Shield Association on behalf of the independent Blue Cross and/or Blue Shield Companies that administer the Federal Employee Program® ("FEP") in their individual locations. The specific name of the Blue Cross and/or Blue Shield Plan to which your FEP membership is assigned is listed on the back of your insurance ID card.

### **What information may have been involved?**

Although we were able to conclude that your personal and health information was accessible to another FEP member during the incident window, we are unable to determine what specific information, if any, was accessed. This is because the information that may have been accessible through the MyBlue Member Portal to another FEP member varied by member. However, the information may have included (1) information to identify and contact you (such as first, middle, and last name, address, phone number(s), email address, group and member ID numbers, and date of birth); (2) information related to medical and/or claims histories (such as medical providers, dates of service, diagnoses, treatment information, test results and medical records); and (3) information regarding prescriptions, including drug name, number, prescriber name and pharmacy name. The incident did not involve access to your Social Security number, full financial account, or credit or debit card numbers.

### **What we are doing.**

As soon as we discovered the incident, we promptly took down the MyBlue Member Portal and launched an investigation. We resolved the issue and then restored the MyBlue Member Portal services. Since resolution, we have not been notified of the issue recurring, although we continue to monitor the Portal for any related issues.

While we are unaware of any misuse of your information as a result of this incident, including your credit or financial information, in an abundance of caution we have nonetheless arranged to offer you credit monitoring and identity restoration services for a period of two years, free of charge through Experian. You have until June 30, 2020 to activate these services, and instructions on how to activate these services are included in the attachments to this letter.

### **What you can do.**

As mentioned above, we are not aware of any misuse of your information to date as a result of this matter. The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to remain vigilant in monitoring your account statements, bills, notices, and insurance transactions for incidents of any unusual or unauthorized activity, and to promptly report such incidents to your health care provider or your local Blue Cross and/or Blue Shield Plan. Additionally, as a proactive step, we encourage you to review your personal information contained on the MyBlue Member Portal.

Blue Cross Blue Shield Association is an association of independent Blue Cross and Blue Shield companies.

**For More Information.**

If you have any questions about this matter or would like additional information, please call the FEP National Information Center toll free at 1-800-411-BLUE (2583) (callers may press #1, then press #0 to speak to a live agent). This call center is open Monday through Friday, 8 a.m. until 8 p.m. Eastern Standard Time, excluding weekends and holidays. We apologize for any concern this event may cause you and we greatly appreciate your understanding.

We regret that this incident occurred. We take the privacy of your personal information with the utmost seriousness and have implemented steps to prevent this in the future.

Sincerely,

A handwritten signature in black ink that reads "William A. Breskin". The signature is written in a cursive style with a large initial 'W' and 'B'.

William A. Breskin  
Senior Vice President, Government Programs

Blue Cross Blue Shield Association is an association of independent Blue Cross and Blue Shield companies.

## Reference Guide

### **Review Your Account Statements**

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for health insurance statements, to your health plan.

### **Provide any updated personal information to your health care provider**

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

### **Order Your Free Credit Report**

To order your free annual credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus (Equifax, Experian and TransUnion) provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

### **How to Enroll in Experian's® IdentityWorks<sup>SM</sup>**

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks<sup>SM</sup>.<sup>1</sup> This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

---

<sup>1</sup> <?> Experian®, IdentityWorks<sup>SM</sup>, and Experian IdentityWorks ExtendCARE™ are trademarks owned by Experian Information Solutions, Inc., an independent global information services company offering consumer credit reporting and a suite of identity detection and identity theft resolution services. Learn more at [www.experianplc.com](http://www.experianplc.com).

- Ensure that you **enroll by: June 30, 2020** (Your code will not work after this date)
- **Visit** the Experian IdentityWorks website to enroll:  
**<https://www.experianidworks.com/credit>**
- Provide your **activation code: [INSERT INDIVIDUAL CODE FROM PIN CODE EXCEL FILE]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **866.579.5479** by **June 30, 2020**. Be prepared to provide engagement number **DB18701** as proof of eligibility for the identity restoration services by Experian.

#### **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 866.579.5479 (be prepared to provide engagement number **DB18701** as proof of eligibility for the identity restoration services by Experian). If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

### **Contact the U.S. Federal Trade Commission**

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

### **Place a Fraud Alert on Your Credit File**

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

### **Security Freezes**

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any

suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Freeze	Security	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	<a href="http://www.equifax.com">www.equifax.com</a>
Experian Freeze	Security	P.O. Box 9554 Allen, TX 75013	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion		P.O. Box 160 Woodlyn, PA 19094	888-909-8872	<a href="http://www.transunion.com">www.transunion.com</a>

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

#### **For Residents of Iowa**

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

Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)

#### **For Residents of Maryland**

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division  
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, <http://www.marylandattorneygeneral.gov/>

#### **For Residents of New Mexico**

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity;
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

#### **For Residents of North Carolina**

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division  
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov)

#### **For Residents of Oregon**

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392,  
[www.doj.state.or.us](http://www.doj.state.or.us)