RECEIVED
15 SEP 11 AM 9:09
CONSUMER PROTECTION DIV.

BakerHostetler

Baker&Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111
T 212.589.4200
F 212.589.4201
www.bakerlaw.com
Theodore J. Kobus III
direct dial: 212.271.1584
tkobus@bakerlaw.com

2015 SEP 10 AM 9:22
ATTORNEY GENERAL

September 9, 2015

***VIA OVERNIGHT DELIVERY***

Office of the Attorney General
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut St.
Des Moines, IA 50319

*Re: Incident Notification*

Dear Sir or Madam:

Our client, The Lifetime Healthcare Companies ("LTHC"), including its affiliates Excellus BlueCross BlueShield ("Excellus BCBS"), Lifetime Health Medical Group, Lifetime Benefit Solutions, Lifetime Care, The MedAmerica Companies ("MedAmerica"), and Univera Healthcare ("Univera"), on August 5, 2015, learned that cyber-attackers had executed a sophisticated attack to gain unauthorized access to its Information Technology (IT) systems. Further investigation revealed that the initial attack occurred on December 23, 2013. LTHC worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct its investigation and to remediate the issues created by the attack on its IT systems. LTHC notified the FBI and continues to work closely with the agency on its investigation.

LTHC's investigation has determined that the attackers may have possibly gained unauthorized access to LTHC's members', patients', and other individuals' personal information, including names, addresses, telephone numbers, dates of birth, Social Security numbers, member identification numbers, financial account information, claims information and, in some instances, clinical information. As to Excellus BCBS, Univera, and MedAmerica, these entities acquire this information in their capacity as health plans, as administrators for self-funded accounts, or as service providers, and in the case of Excellus BCBS, as a participant in the national BlueCard program.[1] In these cases and without waiving any objection to personal jurisdiction or ERISA-

[1] Excellus BCBS participates in the national BlueCard program, which allows a member in one Blue Cross Blue Shield (BCBS) plan to get high-quality affordable health care they need wherever they are from providers that participate in a different BCBS plan's network. If an individual received health care in the 31 county upstate New York service area of Excellus BCBS, health care providers in that area may have shared information with Excellus BCBS in order to process claims.

preemption, this notice is intended to satisfy obligations for Excellus, Univera and MedAmerica, their self-funded accounts and customers, Blue Cross Blue Shield (BCBS) plans and BCBS plans' self-funded accounts to notify your office about this incident.

The investigation has not determined that any such data was removed from LTHC's systems. We also have no evidence to date that such data has been used inappropriately.

Although we know of no reports of identity theft or other fraud related to this incident, LTHC is beginning to notify individuals affected by the incident on September 9, 2015. LTHC is offering affected individuals two years of complimentary identity theft protection services through Kroll, including credit monitoring powered by TransUnion. LTHC also is providing call center support for those affected. In addition, LTHC is recommending that members regularly review their explanation of benefits statements for suspicious activity. Should any member identify a medical service listed on an explanation of benefits statement that was not received, the member should immediately contact LTHC.

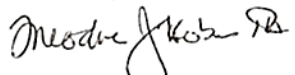
LTHC is notifying Iowa residents in substantially the same form as the letters attached hereto.[2] As covered entities under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the affiliates of LTHC are required to maintain procedures for responding to a breach of security, and notification to Iowa residents who are members is being provided in compliance with these procedures. *See* IOWA CODE ANN. § 715C.2(7)(a); *see also* 45 C.F.R. §§ 160.103 and 164.400 *et seq.*

Notification is being provided in the most expedient time possible and without unreasonable delay pursuant to the investigation described above, which was necessary to determine the scope of the incident; restore the reasonable integrity of the data system; and identify the individuals potentially affected. *See* IOWA CODE ANN. § 715C.2(1).

In addition to remediating its IT systems of the issues raised by this cyberattack and to help prevent something like this from happening in the future, LTHC has taken actions to strengthen and enhance the security of its IT systems moving forward.

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

Sincerely,



Theodore J. Kobus III

Enclosures

[2] This report is not, and does not constitute, a waiver of personal jurisdiction.

Excellus

A nonprofit independent licensee of the Blue Cross Blue Shield Association

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

September 9, 2015

Dear <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you that Excellus BlueCross BlueShield ("Excellus BCBS") was the target of a sophisticated cyberattack, and that some of your personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are fully cooperating with its investigation into this attack.

We at Excellus BCBS take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect you and your information moving forward.

**What happened?**

On August 5, 2015, we learned that cyber attackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on December 23, 2013. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remediate the issues created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your information, which could include your name, address, telephone number, date of birth, Social Security number, member identification number, financial account information, and claims information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

**What is Excellus BCBS doing to protect you?**

We recognize this issue can be frustrating and we are taking steps to protect you. We are providing protection and assistance to those affected by this cyberattack, including two years of free credit monitoring and identity theft protection services.

Specifically, we have secured the services of Kroll to provide identity theft protection at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Your identity theft protection services include Credit Monitoring, Web Watcher, and Identity Theft Consultation and Restoration. **To enroll, visit excellusfacts.com** and follow the online instructions to take advantage of your identity theft protection services.* To receive credit services by mail instead of online, please call 877-589-3331. Additional information describing your services is included with this letter.

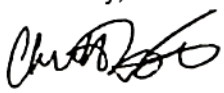
We also recommend that you regularly review the Explanation of Benefits (EOB) statements Excellus BCBS sends you. If you identify medical services listed on your EOB that you did not receive, please contact us immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your bank account or change your bank account number, please contact your bank.

**What have we done to prevent this from happening in the future?**
Along with steps we took to close the vulnerability in our IT system, Excellus BCBS is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

**Where can you get more information on this issue?**
You have two options to obtain more information, online or via phone. **You can visit excellusfacts.com for more information.** Or, call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time (closed on U.S. observed holidays). TTY/TDD users should engage their relay service prior to calling the above referenced number.

I want you to know that protecting your information is incredibly important to us, as is helping you through this situation with the information and support you need.

Sincerely,



Christopher C. Booth
President and Chief Executive Officer

---

* Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## Take Advantage of Your Identity Theft Protection Services

You've been provided with access to services from Kroll. **To enroll, visit excellusfacts.com** and follow the online instructions to take advantage of your identity theft protection services.* To receive credit services by mail instead of online, please call 877-589-3331. The following services are included:

### Web Watcher

Web Watcher monitors internet sites where criminals buy, sell and trade personal identity information, looking for matches of Social Security Numbers, credit/debit card numbers, e-mails, phone numbers, bank account and routing number, and medical identification number. The Member is promptly notified if evidence of their identity information being traded or sold is discovered through such monitoring.

### Credit Monitoring

Credit monitoring is powered by TransUnion. Credit monitoring can be a key tool in detecting early warning signs of identity theft. You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft. You'll also receive "no activity" notices if there have been no changes to your data.

### Consultation and Restoration Services

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

**Consultation:** You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Restoration:** Should you become a victim of identity theft; a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and others to resolve it.

---

* Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## INFORMATION ABOUT PREVENTING IDENTITY THEFT

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

| Equifax | Experian | TransUnion |
|---|---|---|
| PO Box 740241 | PO Box 2002 | PO Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |

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 Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

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

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Excellus

A nonprofit independent licensee of the Blue Cross Blue Shield Association

Parent or Guardian of
<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

September 9, 2015

Dear Parent or Guardian of <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you that Excellus BlueCross BlueShield ("Excellus BCBS") was the target of a sophisticated cyberattack, and that some of your child's personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are fully cooperating with its investigation into this attack.

We at Excellus BCBS take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect your child's information moving forward.

**What happened?**

On August 5, 2015, we learned that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on December 23, 2013. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remediate the issues created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your child's information, which could include your child's name, address, telephone number, date of birth, Social Security number, member identification number, financial account information, and claims information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

**What is Excellus BCBS doing to protect your child?**

We recognize this issue can be frustrating and we are taking steps to protect your child. We are providing protection and assistance to those affected by this cyberattack, including two years of identity theft protection services.

Specifically, we have secured the services of Kroll to provide identity theft protection at no cost to your child for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your child's identity theft protection services include Identity Theft Consultation and Restoration. If you have any questions or feel that your child has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have. Additional information describing your services is included with this letter.

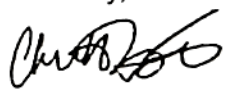
We also recommend that you regularly review the Explanation of Benefits (EOB) statements Excellus BCBS sends in relation to services received by your child. If you identify medical services listed on your EOB that your child did not receive, please contact us immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your child's bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your child's bank account or change your child's bank account number, please contact your child's bank.

**What have we done to prevent this from happening in the future?**
Along with steps we took to close the vulnerability in our IT system, Excellus BCBS is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

**Where can you get more information on this issue?**
You have two options to obtain more information, online or via phone. **You can visit excellusfacts.com for more information.** Or, call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time (closed on U.S. observed holidays). TTY/TDD users should engage their relay service prior to calling the above referenced number.

I want you to know that protecting your information is incredibly important to us, as is helping you through this situation with the information and support you need.

Sincerely,



Christopher C. Booth
President and Chief Executive Officer

## Take Advantage of Your Identity Theft Protection Services

Your child has been provided with the following services from Kroll:

**Consultation and Restoration Services**

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

**Consultation:** You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Restoration:** Should your child become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and others to resolve it.

If you have any questions or feel that your child has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have.

## INFORMATION ABOUT PREVENTING IDENTITY THEFT

In addition, we recommend that you remain vigilant to the possibility of fraud and identity theft over the next 12 to 24 months by reviewing your child's account statements and immediately reporting any suspicious activity to us. You may also obtain a copy of your child's credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your child's credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You should periodically obtain credit reports from each of the nationwide credit reporting agencies and request that any fraudulent activity be deleted. Contact information for the three nationwide credit reporting agencies is as follows:

| Equifax | Experian | TransUnion |
|---|---|---|
| PO Box 740241 | PO Box 2002 | PO Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |

If you believe you or your child is the victim of identity theft or have reason to believe your or your child's personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

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

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your or your child's records.

Excellus

A nonprofit independent licensee of the Blue Cross Blue Shield Association

Estate of
<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

September 9, 2015

Dear Estate of <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you that Excellus BlueCross BlueShield ("Excellus BCBS") was the target of a sophisticated cyberattack, and that some of your family member's personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are fully cooperating with its investigation into this attack.

We at Excellus BCBS take this issue seriously and regret the concern it may cause. Our regret is compounded by the fact that we know you lost your family member, which may make this more difficult to receive. I'm writing to provide you information on the steps we are taking to protect your family member's information moving forward.

**What happened?**

On August 5, 2015, we learned that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on December 23, 2013. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remediate the issues created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your family member's information, which could include your family member's name, address, telephone number, date of birth, Social Security number, member identification number, financial account information, and claims information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

**What is Excellus BCBS doing to protect your family member?**

We recognize this issue can be frustrating and we are taking steps to protect your family member. We are providing protection and assistance to those affected by this cyberattack, including two years of identity theft protection services.

Specifically, we have secured the services of Kroll to provide identity theft protection at no cost to your family member for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your family member's identity theft protection services include Identity Theft Consultation and Restoration. If you have any questions or feel that your family member has an

identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have. Additional information describing your services is included with this letter.

If you still receive Explanation of Benefits (EOB) statements from Excellus BCBS regarding your family member, we recommend that you review them. If you identify medical services listed on the EOB that your family member did not receive, please contact us immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your family member's bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your family member's bank account or change your family member's bank account number, please contact your family member's bank.

**What have we done to prevent this from happening in the future?**
Along with steps we took to close the vulnerability in our IT system, Excellus BCBS is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

**Where can you get more information on this issue?**
You have two options to obtain more information, online or via phone. **You can visit excellusfacts.com for more information.** Or, call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time (closed on U.S. observed holidays). TTY/TDD users should engage their relay service prior to calling the above referenced number.

I want you to know that protecting your information is incredibly important to us, as is helping you through this situation with the information and support you need.

Sincerely,

Christopher C. Booth
President and Chief Executive Officer

## Take Advantage of Your Identity Theft Protection Services

Your family member has been provided with the following services from Kroll:

**Consultation and Restoration Services**

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

**Consultation:** You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Restoration:** Should your family member become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and others to resolve it.

If you have any questions or feel that your family member has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have.

The Lifetime Healthcare Companies

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

September 9, 2015

Dear <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you that The Lifetime Healthcare Companies ("LTHC"), including its affiliates Lifetime Benefit Solutions, Lifetime Care, Lifetime Health Medical Group, The MedAmerica Companies, and Univera Healthcare, was the target of a sophisticated cyberattack, and that some of your personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are fully cooperating with its investigation into this attack.

We take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect you and your information moving forward.

**What affiliates are impacted?**
You are receiving this notification letter because you received services from one or more of the following affected affiliates:

- *Lifetime Benefit Solutions* - Provides employee benefits administration and risk management services, including flexible spending account, 401k and health reimbursement account administration, benefits consulting and administrative support, across the United States.
- *Lifetime Care* - Delivers compassionate, personalized care and education to adults and children who are ill, injured, dying, or grieving.
- *Lifetime Health Medical Group* - Delivers primary care, specialty care, urgent care, pharmacy, dental, optical, behavioral health, and imaging services in the Rochester and Buffalo areas.
- *The MedAmerica Companies* - A group of carriers who underwrite and administer long term care insurance nationally under the names MedAmerica Insurance Company, MedAmerica Insurance Company of New York, MedAmerica Insurance Company of Florida, and who also provide third party administrative services to other insurers across the country.
- *Univera Healthcare* - Covers members across the eight counties of Western New York with a wide array of health plans and services, including a comprehensive network of physicians, hospitals, and all major pharmacy chains.

**What happened?**
On August 5, 2015, we learned that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on December 23, 2013. We worked closely with Mandiant, one of

the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your information, which could include your name, address, telephone number, date of birth, Social Security number, member identification number, financial account information, claims information and, in some instances, clinical information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

**What are we doing to protect you?**
We recognize this issue can be frustrating and we are taking steps to protect you. We are providing protection and assistance to those affected by this cyberattack, including two years of free credit monitoring and identity theft protection services.

Specifically, we have secured the services of Kroll to provide identity theft protection at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity theft protection services include Credit Monitoring, Web Watcher, and Identity Theft Consultation and Restoration. **To enroll, visit lifethcfacts.com** and follow the online instructions to take advantage of your identity theft protection services.* Additional information describing your services is included with this letter.

We also recommend that you regularly review the Explanation of Benefits (EOB) statements your health insurer sends you. If you identify medical services listed on your EOB that you did not receive, please contact your health insurer immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your bank account or change your bank account number, please contact your bank.

**What have we done to prevent this from happening in the future?**
Along with steps we took to close the vulnerability in our IT system, we are taking additional actions to strengthen and enhance the security of our IT systems moving forward.

**Where can you get more information on this issue?**
You have two options to obtain more information, online or via phone. **You can visit lifethcfacts.com for more information.** Or, call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time (closed on U.S. observed holidays). TTY/TDD users should engage their relay service prior to calling the above referenced number.

I want you to know that protecting your information is incredibly important to us, as is helping you through this situation with the information and support you need.

Sincerely,

Christopher C. Booth
President and Chief Executive Officer

---

* Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## Take Advantage of Your Identity Theft Protection Services

You've been provided with access to services from Kroll. **To enroll, visit lifethcfacts.com** and follow the online instructions to take advantage of your identity theft protection services.* To receive credit services by mail instead of online, please call 877-589-3331. The following services are included:

### Web Watcher

Web Watcher monitors internet sites where criminals buy, sell and trade personal identity information, looking for matches of Social Security Numbers, credit/debit card numbers, e-mails, phone numbers, bank account and routing number, and medical identification number. The Member is promptly notified if evidence of their identity information being traded or sold is discovered through such monitoring.

### Credit Monitoring

Credit monitoring is powered by TransUnion. Credit monitoring can be a key tool in detecting early warning signs of identity theft. You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft. You'll also receive "no activity" notices if there have been no changes to your data.

### Consultation and Restoration Services

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

**Consultation:** You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Restoration:** Should you become a victim of identity theft; a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and others to resolve it.

---

* Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## INFORMATION ABOUT PREVENTING IDENTITY THEFT

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

| Equifax | Experian | TransUnion |
|---|---|---|
| PO Box 740241 | PO Box 2002 | PO Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |

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 Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

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

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

The Lifetime Healthcare Companies

Parent or Guardian of
<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

September 9, 2015

Dear Parent or Guardian of <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you that The Lifetime Healthcare Companies ("LTHC"), including its affiliates Lifetime Benefit Solutions, Lifetime Care, Lifetime Health Medical Group, The MedAmerica Companies, and Univera Healthcare, was the target of a sophisticated cyberattack, and that some of your child's personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are fully cooperating with its investigation into this attack.

We take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect your child's information moving forward.

**What affiliates are impacted?**
You are receiving this notification letter because your child received services from one or more of the following affected affiliates:

- *Lifetime Benefit Solutions* - Provides employee benefits administration and risk management services, including flexible spending account, 401k and health reimbursement account administration, benefits consulting and administrative support, across the United States.
- *Lifetime Care* - Delivers compassionate, personalized care and education to adults and children who are ill, injured, dying, or grieving.
- *Lifetime Health Medical Group* - Delivers primary care, specialty care, urgent care, pharmacy, dental, optical, behavioral health, and imaging services in the Rochester and Buffalo areas.
- *The MedAmerica Companies* - A group of carriers who underwrite and administer long term care insurance nationally under the names MedAmerica Insurance Company, MedAmerica Insurance Company of New York, MedAmerica Insurance Company of Florida, and who also provide third party administrative services to other insurers across the country.
- *Univera Healthcare* - Covers members across the eight counties of Western New York with a wide array of health plans and services, including a comprehensive network of physicians, hospitals, and all major pharmacy chains.

**What happened?**
On August 5, 2015, we learned that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on December 23, 2013. We worked closely with Mandiant, one of

the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your child's information, which could include your child's name, address, telephone number, date of birth, Social Security number, member identification number, financial account information, claims information and, in some instances, clinical information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

**What are we doing to protect your child?**
We recognize this issue can be frustrating and we are taking steps to protect your child. We are providing protection and assistance to those affected by this cyberattack, including two years of free identity theft protection services.

Specifically, we have secured the services of Kroll to provide identity theft protection at no cost to your child for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your child's identity theft protection services include Identity Theft Consultation and Restoration. If you have any questions or feel that your child has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have. Additional information describing your services is included with this letter.

We also recommend that you regularly review the Explanation of Benefits (EOB) statements that your health plan sends in relation to services received by your child. If you identify medical services listed on your EOB that your child did not receive, please contact your health plan immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your child's bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your child's bank account or change your child's bank account number, please contact your child's bank.

**What have we done to prevent this from happening in the future?**
Along with steps we took to close the vulnerability in our IT system, we are taking additional actions to strengthen and enhance the security of our IT systems moving forward.

**Where can you get more information on this issue?**
You have two options to obtain more information, online or via phone. **You can visit lifethcfacts.com for more information.** Or, call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time (closed on U.S. observed holidays). TTY/TDD users should engage their relay service prior to calling the above referenced number.

I want you to know that protecting your information is incredibly important to us, as is helping you through this situation with the information and support you need.

Sincerely,

Christopher C. Booth
President and Chief Executive Officer

## Take Advantage of Your Identity Theft Protection Services

Your child has been provided with the following services from Kroll:

**Consultation and Restoration Services**

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

**Consultation:** You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Restoration:** Should your child become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and others to resolve it.

If you have any questions or feel that your child has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have.

## INFORMATION ABOUT PREVENTING IDENTITY THEFT

In addition, we recommend that you remain vigilant to the possibility of fraud and identity theft over the next 12 to 24 months by reviewing your child's account statements and immediately reporting any suspicious activity to us. You may also obtain a copy of your child's credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your child's credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You should periodically obtain credit reports from each of the nationwide credit reporting agencies and request that any fraudulent activity be deleted. Contact information for the three nationwide credit reporting agencies is as follows:

| Equifax | Experian | TransUnion |
|---|---|---|
| PO Box 740241 | PO Box 2002 | PO Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |

If you believe you or your child is the victim of identity theft or have reason to believe your or your child's personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

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

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your or your child's records.

The Lifetime Healthcare Companies

Estate of
<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

September 9, 2015

Dear Estate of <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you that The Lifetime Healthcare Companies ("LTHC"), including its affiliates Lifetime Benefit Solutions, Lifetime Care, Lifetime Health Medical Group, The MedAmerica Companies, and Univera Healthcare, was the target of a sophisticated cyberattack, and that some of your family member's personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are fully cooperating with its investigation into this attack.

We take this issue seriously and regret the concern it may cause. Our regret is compounded by the fact that we know you lost your family member, which may make this more difficult to receive. I'm writing to provide you information on the steps we are taking to protect your family member's information moving forward.

**What affiliates are impacted?**
You are receiving this notification letter because your family member received services from one or more of the following affected affiliates:

- *Lifetime Benefit Solutions* - Provides employee benefits administration and risk management services, including flexible spending account, 401k and health reimbursement account administration, benefits consulting and administrative support, across the United States.
- *Lifetime Care* - Delivers compassionate, personalized care and education to adults and children who are ill, injured, dying, or grieving.
- *Lifetime Health Medical Group* - Delivers primary care, specialty care, urgent care, pharmacy, dental, optical, behavioral health, and imaging services in the Rochester and Buffalo areas.
- *The MedAmerica Companies* - A group of carriers who underwrite and administer long term care insurance nationally under the names MedAmerica Insurance Company, MedAmerica Insurance Company of New York, MedAmerica Insurance Company of Florida, and who also provide third party administrative services to other insurers across the country.
- Univera Healthcare - Covers members across the eight counties of Western New York with a wide array of health plans and services, including a comprehensive network of physicians, hospitals, and all major pharmacy chains.

**What happened?**
On August 5, 2015, we learned that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed

that the initial attack occurred on December 23, 2013. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your family member's information, which could include your family member's name, address, telephone number, date of birth, Social Security number, member identification number, financial account information, claims information and, in some instances, clinical information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

**What are we doing to protect your family member?**
We recognize this issue can be frustrating and we are taking steps to protect your family member. We are providing protection and assistance to those affected by this cyberattack, including two years of identity theft protection services.

Specifically, we have secured the services of Kroll to provide identity theft protection at no cost to your family member for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your family member's identity theft protection services include Identity Theft Consultation and Restoration. If you have any questions or feel that your family member has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have. Additional information describing your services is included with this letter.

If you still receive Explanation of Benefits (EOB) statements from your family member's health plan regarding your family member, we recommend that you review them. If you identify medical services listed on the EOB that your family member did not receive, please contact your family member's health plan immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your family member's bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your family member's bank account or change your family member's bank account number, please contact your family member's bank.

**What have we done to prevent this from happening in the future?**
Along with steps we took to close the vulnerability in our IT system, we are taking additional actions to strengthen and enhance the security of our IT systems moving forward.

**Where can you get more information on this issue?**
You have two options to obtain more information, online or via phone. **You can visit lifethcfacts.com for more information**. Or, call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time (closed on U.S. observed holidays). TTY/TDD users should engage their relay service prior to calling the above referenced number.

I want you to know that protecting your information is incredibly important to us, as is helping you through this situation with the information and support you need.

Sincerely,

Christopher C. Booth
President and Chief Executive Officer

## Take Advantage of Your Identity Theft Protection Services

Your family member has been provided with the following services from Kroll:

**Consultation and Restoration Services**

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

**Consultation:** You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Restoration:** Should your family member become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and others to resolve it.

If you have any questions or feel that your family member has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have.

Excellus

A nonprofit independent licensee of the Blue Cross Blue Shield Association

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

September 9, 2015

Dear <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you that Excellus BlueCross BlueShield ("Excellus BCBS") was the target of a sophisticated cyberattack, and that some of your personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are fully cooperating with its investigation into this attack.

We at Excellus BCBS take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect you and your information moving forward.

**What happened?**

On August 5, 2015, we learned that cyber attackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on December 23, 2013. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remediate the issues created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your information, which could include your name, address, telephone number, date of birth, Social Security number, member identification number, financial account information, and claims information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

**Why does Excellus BCBS have your information?**

We believe you have or had health plan coverage through another independent Blue Cross Blue Shield (BCBS) plan, and that you may have received services in the 31 county upstate New York service area of Excellus BCBS. Excellus BCBS is a service provider in 31 upstate New York counties to BCBS plans across the country.

**What is Excellus BCBS doing to protect you?**

We recognize this issue can be frustrating and we are taking steps to protect you. We are providing protection and assistance to those affected by this cyberattack, including two years of free credit monitoring and identity theft protection services.

Specifically, we have secured the services of Kroll to provide identity theft protection at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity theft protection services include Credit Monitoring, Web Watcher, and Identity Theft Consultation and Restoration. **To enroll, visit excellusfacts.com** and follow the online instructions to take advantage of your identity theft protection services.* To receive credit services by mail instead of online, please call 877-589-3331. Additional information describing your services is included with this letter.

We also recommend that you regularly review the Explanation of Benefits (EOB) statements that your health plan sends you. If you identify medical services listed on your EOB that you did not receive, please contact your health plan immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your bank account or change your bank account number, please contact your bank.

**What have we done to prevent this from happening in the future?**
Along with steps we took to close the vulnerability in our IT system, Excellus BCBS is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

**Where can you get more information on this issue?**
You have two options to obtain more information, online or via phone. **You can visit excellusfacts.com for more information.** Or, call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time (closed on U.S. observed holidays). TTY/TDD users should engage their relay service prior to calling the above referenced number.

I want you to know that protecting your information is incredibly important to us, as is helping you through this situation with the information and support you need.

Sincerely,

Christopher C. Booth
President and Chief Executive Officer

---

* Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## Take Advantage of Your Identity Theft Protection Services

You've been provided with access to services from Kroll. **To enroll, visit excellusfacts.com** and follow the online instructions to take advantage of your identity theft protection services.* To receive credit services by mail instead of online, please call 877-589-3331. The following services are included:

### Web Watcher

Web Watcher monitors internet sites where criminals buy, sell and trade personal identity information, looking for matches of Social Security Numbers, credit/debit card numbers, e-mails, phone numbers, bank account and routing number, and medical identification number. The Member is promptly notified if evidence of their identity information being traded or sold is discovered through such monitoring.

### Credit Monitoring

Credit monitoring is powered by TransUnion. Credit monitoring can be a key tool in detecting early warning signs of identity theft. You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft. You'll also receive "no activity" notices if there have been no changes to your data.

### Consultation and Restoration Services

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

**Consultation:** You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Restoration:** Should you become a victim of identity theft; a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and others to resolve it.

---

* Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## INFORMATION ABOUT PREVENTING IDENTITY THEFT

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

| Equifax | Experian | TransUnion |
|---|---|---|
| PO Box 740241 | PO Box 2002 | PO Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |

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 Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

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

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Excellus

A nonprofit independent licensee of the Blue Cross Blue Shield Association

Parent or Guardian of
<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

September 9, 2015

Dear Parent or Guardian of <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you that Excellus BlueCross BlueShield ("Excellus BCBS") was the target of a sophisticated cyberattack, and that some of your child's personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are fully cooperating with its investigation into this attack.

We at Excellus BCBS take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect your child's information moving forward.

**What happened?**
On August 5, 2015, we learned that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on December 23, 2013. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remediate the issues created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your child's information, which could include your child's name, address, telephone number, date of birth, Social Security number, member identification number, financial account information, and claims information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

**Why does Excellus BCBS have your child's information?**
We believe your child has or had health plan coverage through another independent Blue Cross Blue Shield (BCBS) plan, and that your child may have received services in the 31 county upstate New York service area of Excellus BCBS. Excellus BCBS is a service provider in 31 upstate New York counties to BCBS plans across the country.

**What is Excellus BCBS doing to protect your child?**
We recognize this issue can be frustrating and we are taking steps to protect your child. We are providing protection and assistance to those affected by this cyberattack, including two years of identity theft protection services.

Specifically, we have secured the services of Kroll to provide identity theft protection at no cost to your child for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your child's identity theft protection services include Identity Theft Consultation and Restoration. If you have any questions or feel that your child has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have. Additional information describing your services is included with this letter.

We also recommend that you regularly review the Explanation of Benefits (EOB) statements that your health plan sends in relation to services received by your child. If you identify medical services listed on your EOB that your child did not receive, please contact your health plan immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your child's bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your child's bank account or change your child's bank account number, please contact your child's bank.

**What have we done to prevent this from happening in the future?**
Along with steps we took to close the vulnerability in our IT system, Excellus BCBS is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

**Where can you get more information on this issue?**
You have two options to obtain more information, online or via phone. **You can visit excellusfacts.com for more information.** Or, call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time (closed on U.S. observed holidays). TTY/TDD users should engage their relay service prior to calling the above referenced number.

I want you to know that protecting your information is incredibly important to us, as is helping you through this situation with the information and support you need.

Sincerely,

Christopher C. Booth
President and Chief Executive Officer

## Take Advantage of Your Identity Theft Protection Services

Your child has been provided with the following services from Kroll:

**Consultation and Restoration Services**

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

**Consultation:** You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Restoration:** Should your child become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and others to resolve it.

If you have any questions or feel that your child has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have.

## INFORMATION ABOUT PREVENTING IDENTITY THEFT

In addition, we recommend that you remain vigilant to the possibility of fraud and identity theft over the next 12 to 24 months by reviewing your child's account statements and immediately reporting any suspicious activity to us. You may also obtain a copy of your child's credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your child's credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You should periodically obtain credit reports from each of the nationwide credit reporting agencies and request that any fraudulent activity be deleted. Contact information for the three nationwide credit reporting agencies is as follows:

| Equifax | Experian | TransUnion |
|---|---|---|
| PO Box 740241 | PO Box 2002 | PO Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |

If you believe you or your child is the victim of identity theft or have reason to believe your or your child's personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

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

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your or your child's records.

Excellus

A nonprofit independent licensee of the Blue Cross Blue Shield Association

Estate of
<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

September 9, 2015

Dear Estate of <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you that Excellus BlueCross BlueShield ("Excellus BCBS") was the target of a sophisticated cyberattack, and that some of your family member's personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are fully cooperating with its investigation into this attack.

We at Excellus BCBS take this issue seriously and regret the concern it may cause. Our regret is compounded by the fact that we know you lost your family member, which may make this more difficult to receive. I'm writing to provide you information on the steps we are taking to protect your family member's information moving forward.

**What happened?**
On August 5, 2015, we learned that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on December 23, 2013. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remediate the issues created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your family member's information, which could include your family member's name, address, telephone number, date of birth, Social Security number, member identification number, financial account information, and claims information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

**Why does Excellus BCBS have your family member's information?**
We believe your family member had health plan coverage through another independent Blue Cross Blue Shield (BCBS) plan, and that your family member may have received services in the 31 county upstate New York service area of Excellus BCBS. Excellus BCBS is a service provider in 31 upstate New York counties to BCBS plans across the country.

**What is Excellus BCBS doing to protect your family member?**
We recognize this issue can be frustrating and we are taking steps to protect your family member. We are providing protection and assistance to those affected by this cyberattack, including two years of identity theft protection services.

Specifically, we have secured the services of Kroll to provide identity theft protection at no cost to your family member for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your family member's identity theft protection services include Identity Theft Consultation and Restoration. If you have any questions or feel that your family member has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have. Additional information describing your services is included with this letter.

If you still receive Explanation of Benefits (EOB) statements from your family member's health plan regarding your family member, we recommend that you review them. If you identify medical services listed on the EOB that your family member did not receive, please contact your family member's health plan immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your family member's bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your family member's bank account or change your family member's bank account number, please contact your family member's bank.

**What have we done to prevent this from happening in the future?**
Along with steps we took to close the vulnerability in our IT system, Excellus BCBS is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

**Where can you get more information on this issue?**
You have two options to obtain more information, online or via phone. **You can visit excellusfacts.com for more information.** Or, call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time (closed on U.S. observed holidays). TTY/TDD users should engage their relay service prior to calling the above referenced number.

I want you to know that protecting your information is incredibly important to us, as is helping you through this situation with the information and support you need.

Sincerely,

Christopher C. Booth
President and Chief Executive Officer

## Take Advantage of Your Identity Theft Protection Services

Your family member has been provided with the following services from Kroll:

**Consultation and Restoration Services**

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

**Consultation:** You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Restoration:** Should your family member become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and others to resolve it.

If you have any questions or feel that your family member has an identity theft issue, please call 877-589-3331, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have.