MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 30, 2023

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

To Whom It May Concern:

We represent Imagine360, LLC ("Imagine360") located at 1550 Liberty Ridge Dr #330, Wayne, PA 19087, and are writing on behalf of Imagine360 and its applicable business associates and data owners to notify your office of an incident that may affect the security of certain personal information relating to eighty-two (82) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Imagine360 does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around January 30, 2023, Imagine360 identified unusual activity within a third-party file sharing platform, Citrix, used by Imagine360 to securely exchange files related to self-insured health plans. In response, Imagine360 terminated access to the platform, reset passwords, and confirmed the security of its environment since the platform is externally hosted outside of the Imagine360 environment. In conjunction with these efforts, Imagine360 promptly launched an investigation to determine the full nature and scope of the activity. During the course of this investigation, on or around February 3, 2023, Fortra, a third-party vendor who owns and manages another third-party file sharing platform used by Imagine360, GoAnywhere, notified Imagine360 of a data security incident involving this platform.

According to Fortra, an unauthorized actor copied data maintained in this platform belonging to multiple organizations, including Imagine360. In response, Imagine360 worked with Fortra to

gather more information regarding the full nature and scope of this incident, since the platform is also externally hosted outside of the Imagine360 environment. In addition to this, Imagine360 decided to conduct its own internal investigation into the incident to confirm the full scope of the incidents. Through its investigation of both incidents, Imagine360 learned files were copied from both platforms between January 28 and January 30, 2023.

Imagine360 subsequently confirmed the scope of files copied from both platforms and then worked to understand what information was present in the files and to whom it related, which involved a time intensive and detailed review. On or around June 1, 2023, Imagine360 determined that the information present in the relevant files included information associated with the health insurance claims Imagine360 processes for individual plan members on behalf of other organizations.

The information identified in the impacted files included

After identifying the involved organizations and third-party administrators whose plan and plan members were impacted, Imagine360 provided them notice of the facts described above beginning June 5, 2023. Included in this notice was an offer to notify impacted individuals.

Notice to New Hampshire Residents

On or about June 30, 2023, Imagine360 began providing written notice of this incident to eighty-two (82) impacted plan members residing in New Hampshire. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Notice is also being posted to Imagine360's website and being provided to statewide media.

Other Steps Taken and To Be Taken

Upon discovering the incidents, Imagine360 moved quickly to investigate and respond to the incidents, assess the security of Imagine360 systems, and identify potentially affected individuals. Further, Imagine360 notified federal law enforcement and applicable state insurance authorities regarding the incidents. Imagine360 also suspended use of the GoAnywhere platform and implemented additional safeguards after reviewing its existing policies, processes, and security measures.

Imagine360 is providing access to credit monitoring services through IDX to individuals, whose personal information was potentially affected by these incidents, at no cost to these individuals.

Additionally, Imagine360 is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Imagine360 is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements, and explanation of benefits along with monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Imagine360 is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Imagine360 is also notifying the U.S. Department of Health and Human Services, and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of these incidents, please contact us at

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/cml
Enclosure

EXHIBIT A

imagine360

Return to IDX:
PO Box 480149
Niles, IL 60714

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

June 30, 2023

[Variable 1]

Dear <<Name 1>> <<Name 2>>:

Imagine360, LLC ("Imagine360") is writing to provide you with notice of data security incidents that may impact the confidentiality and security of your information. Imagine360 works with [Variable 2] to process claims associated with your health insurance plan. This letter contains information about the incidents, our response, and steps you can take to better protect your information, should you feel it is appropriate to do so.

What Happened? On or around January 30, 2023, Imagine360 identified unusual activity within a third-party file sharing platform, Citrix. Citrix is used by Imagine360 to securely exchange files related to self-insured health plans. In response, Imagine360 terminated access to the platform, reset passwords, and confirmed the security of its environment since the platform is externally hosted outside of the Imagine360 environment.

In conjunction with these efforts, Imagine360 promptly launched an investigation to determine the full nature and scope of the activity. During the course of this investigation, on or around February 3, 2023, Fortra, a third-party vendor who owns and manages another third-party file sharing platform used by Imagine360 notified Imagine360 of a data security incident. According to Fortra, an unauthorized actor copied data maintained in this platform belonging to multiple organizations, including Imagine360.

In response, Imagine360 worked with Fortra to gather more information regarding the full nature and scope of this incident, since the platform is also externally hosted outside of the Imagine360 environment. In addition to this, Imagine360 decided to conduct its own internal investigation into the incident to confirm the full scope of the incidents. Through its investigation of both incidents, Imagine360 learned files were copied from both platforms between January 28 and January 30, 2023. Imagine360 then confirmed the scope of files copied from both platforms and then worked to understand what information was present in the files and to whom it related, which involved a time intensive and detailed review. You are receiving this letter because we determined on June 1, 2023, that your information was present in the relevant files.

What Information Was Involved? Based on our investigation to date, we determined that the personal information present in the relevant files may include

What We Are Doing. Imagine360 takes these incidents and the privacy of information in its care seriously. We conducted a diligent investigation to confirm the full nature and scope of these incidents. We also took prompt steps to ensure that the incidents did not impact Imagine360's internal systems while conducting a comprehensive review of the information potentially affected. We also reported these incidents to federal law enforcement and will be notifying applicable state and federal regulators.

Further, as part of our ongoing commitment to the privacy and security of information in our care, we suspended use of Fortra's platform and implemented additional safeguards to our existing policies, processes, and security measures. As an added precaution, we are providing you with access to identity monitoring services for at no cost to you. Information on these services and instructions on how to activate may be found in the enclosed *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits along with monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please go to https://response.idx.us/imagine360, scan the QR image, or contact our dedicated call center at (888) 220-5801, Monday through Friday, from 6 a.m. - 6 p.m. Pacific Time (excluding U.S. holidays).

We regret any inconvenience caused by this incident.

Sincerely,

Imagine360

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

Website and Enrollment. and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

IDX representatives are available Monday through Friday from 6 a.m. - 6 p.m. Pacific Time (excluding U.S. holidays). Please note the deadline to enroll is September 30, 2023.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1- 410-576-6300 or 1-888-743-0023; and www.marylandattorneygeneral.gov/. Imagine360 is located at 1550 Liberty Ridge Dr. Suite 330 Wayne, PA 19087.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to these incidents. There are 81 Rhode Island residents impacted by these incidents.

imagine360

Return to IDX:
PO Box 480149
Niles, IL 60714

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

June 30, 2023

[Variable 1]

Dear <<Name 1>> <<Name 2>>:

Imagine360, LLC ("Imagine360") is writing to provide you with notice of a data security incident that may impact the confidentiality and security of your information. Imagine360 works with [Variable 2] to process claims associated with your health insurance plan. This letter contains information about the incident, our response, and steps you can take to better protect your information, should you feel it is appropriate to do so.

What Happened? On or around February 3, 2023, Fortra, a third-party vendor who owns and manages a third-party file sharing platform used by Imagine360 to securely exchange files related to your health plan, notified Imagine360 of a data security incident. According to Fortra, an unauthorized actor(s) copied data maintained in this platform belonging to multiple organizations, including Imagine360, between January 28, 2023, and January 30, 2023. In response, Imagine360 worked with Fortra to gather more information regarding the full nature and scope of this incident, since the platform is externally hosted outside of the Imagine360 environment.

In addition to this, we conducted our own internal investigation to confirm the full scope of incident and to confirm the security of our network. We then completed a time intensive and detailed review of all files potentially affected by this incident to determine what information is present and to whom it relates. You are receiving this letter because we determined on June 1, 2023, that your information was present in the relevant files.

What Information Was Involved? Based on our investigation to date, we determined that the personal information present in the relevant files may include

What We Are Doing. Imagine360 takes this incident and the privacy of information in its care seriously and conducted a diligent investigation to confirm the full nature and scope of the incident. In response to this incident, we took prompt steps to ensure that the incident did not impact Imagine360's internal systems while conducting a comprehensive review of the information potentially affected by this incident. We also reported this incident to federal law enforcement and will be notifying applicable state and federal regulators.

Further, as part of our ongoing commitment to the privacy and security of information in our care, we suspended use of platform and implemented additional safeguards to our existing policies, processes, and security measures. As an added precaution, we are providing you with access to identity monitoring services for at no cost to you. Information on these services and instructions on how to activate may be found in the enclosed *Steps You Can Take to Help Protect Personal Information.*

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits along with monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Personal Information.*

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please go to https://response.idx.us/imagine360, scan the QR image, or contact our dedicated call center at Monday through Friday, from 6 a.m. - 6 p.m. Pacific Time (excluding U.S. holidays).

We regret any inconvenience caused by this incident.

Sincerely,

Imagine360

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Website and Enrollment. and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

IDX representatives are available Monday through Friday from 6 a.m. - 6 p.m. Pacific Time (excluding U.S. holidays). Please note the deadline to enroll is September 30, 2023.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1- 410-576-6300 or 1-888-743-0023; and www.marylandattorneygeneral.gov/. Imagine360 is located at 1550 Liberty Ridge Dr. Suite 330 Wayne, PA 19087.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to these incidents. There are 81 Rhode Island residents impacted by this incident.

imagine360

Return to IDX:
PO Box 480149
Niles, IL 60714

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

June 30, 2023

[Variable 1]

Dear <<Name 1>> <<Name 2>>:

Imagine360, LLC ("Imagine360") is writing to provide you with notice of a data security incident that may impact the confidentiality and security of your information. Imagine360 works with [Variable 2] to process claims associated with your health insurance plan. This letter contains information about the incident, our response, and steps you can take to better protect your information, should you feel it is appropriate to do so.

What Happened? On or around January 30, 2023, Imagine360 identified unusual activity within a third-party file sharing platform, Citrix. Citrix is used by Imagine360 to securely exchange files related to self-insured health plans. In response, Imagine360 terminated access to the third-party file share, reset passwords, and confirmed the security of its environment since the platform is externally hosted outside of the Imagine360 environment. In conjunction with these efforts, Imagine360 promptly launched an investigation to determine the full nature and scope of the activity. Through this investigation, Imagine360 learned that certain files were copied from the platform between January 28 and January 30, 2023, as part of a cyber incident. As such, we completed a time intensive and detailed review of all files potentially affected by this incident to determine what information was present in the files and to whom it relates. You are receiving this letter because we determined on June 1, 2023, that your information was present in the relevant files.

What Information Was Involved? Based on our investigation to date, we determined that the personal information present in the relevant files may

What We Are Doing. Imagine360 takes this incident and the privacy of information in its care seriously and conducted a diligent investigation to confirm the full nature and scope of the incident. In response to this incident, we took prompt steps to ensure that the incident did not impact Imagine360's internal systems while conducting a comprehensive review of the information potentially affected by this incident. We also reported this incident to federal law enforcement and will be notifying applicable state and federal regulators.

Further, as part of our ongoing commitment to the privacy and security of information in our care, we implemented additional safeguards to our existing policies, processes, and security measures. As an added precaution, we are providing you with access to identity monitoring services for at no cost to you. Information on these services and instructions on how to activate may be found in the enclosed *Steps You Can Take to Help Protect Personal Information.*

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits along with monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Personal Information.*

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions,

Monday through Friday, from 6 a.m. - 6 p.m. Pacific Time (excluding U.S. holidays).

We regret any inconvenience caused by this incident.

Sincerely,

Imagine360

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Identity Monitoring and Restoration

Website and Enrollment. and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

IDX representatives are available Monday through Friday from 6 a.m. - 6 p.m. Pacific Time (excluding U.S. holidays). Please note the deadline to

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.