



Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

**City of St. Helena
Administrative Services**

1088 College Ave.
St. Helena, CA 94574
cityofsthelena.org



August 23, 2024

Notice of Data Breach

Dear [REDACTED]:

On behalf of The City of St. Helena, I am writing to inform you of an incident involving unauthorized access to some of your information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On May 13, 2024, we detected unauthorized activity on our network. We promptly began investigating to determine the scope of the incident and working with cybersecurity experts on remediation. Once we identified the impacted data, we engaged a data-review firm to review the content of those files. We received those results on August 7, 2024, and promptly determined which individuals to notify.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that an unauthorized third party accessed materials on our network containing your personal information, including your name, contact information, date of birth, and limited medical information (such as treatment details, insurance information, or similar records we received).

WHAT WE ARE DOING

We hired third-party experts to help us address this situation. They investigated the unauthorized activity and worked with us to further secure our systems.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity. Please also review the next page for steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at 888-453-9048 Monday through Friday 9:00 am - 7:00 pm Eastern, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Mandy Kellogg
Administrative Services Administrator

HELENA-ADT-M

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**North Carolina
Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

**Washington, DC
Attorney General**
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

**City of St. Helena
Administrative Services**

1088 College Ave.
St. Helena, CA 94574
cityofsthelena.org



August 23, 2024

Notice of Data Breach

Dear [REDACTED]:

On behalf of The City of St. Helena, I am writing to inform you of an incident involving unauthorized access to some of your information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On May 13, 2024, we detected unauthorized activity on our network. We promptly began investigating to determine the scope of the incident and working with cybersecurity experts on remediation. Once we identified the impacted data, we engaged a data-review firm to review the content of those files. We received those results on August 7, 2024, and promptly determined which individuals to notify.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that an unauthorized third party accessed materials on our network containing your personal information, including your name, contact information, date of birth, and government identification number (such as a passport number, driver's license number, or Social Security number).

WHAT WE ARE DOING

We hired third-party experts to help us address this situation. They investigated the unauthorized activity and worked with us to further secure our systems.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity, and we are offering a complimentary 12-month membership to Experian's IdentityWorks. Please also review the next page for steps to enroll in IdentityWorks and for other steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at 888-453-9048 Monday through Friday 9:00 am - 7:00 pm Eastern, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Mandy Kellogg
Administrative Services Administrator

HELENA-ADT-CM

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary 12-month membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: 11/15/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** [REDACTED]

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **11/15/2024**, and provide them engagement number [REDACTED].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**North Carolina
Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

**Washington, DC
Attorney General**
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

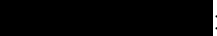
**City of St. Helena
Administrative Services**

1088 College Ave.
St. Helena, CA 94574
cityofsthelena.org



August 23, 2024

Notice of Data Breach

Dear :

On behalf of The City of St. Helena, I am writing to inform you of an incident involving unauthorized access to some of your information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On May 13, 2024, we detected unauthorized activity on our network. We promptly began investigating to determine the scope of the incident and working with cybersecurity experts on remediation. Once we identified the impacted data, we engaged a data-review firm to review the content of those files. We received those results on August 7, 2024, and promptly determined which individuals to notify.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that an unauthorized third party accessed materials on our network containing your personal information, including your name, contact information, date of birth, and government identification number (such as a passport number, driver's license number, or Social Security number).

WHAT WE ARE DOING

We hired third-party experts to help us address this situation. They investigated the unauthorized activity and worked with us to further secure our systems.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity, and we are offering a complimentary 12-month membership to Experian's IdentityWorks. Please also review the next page for steps to enroll in IdentityWorks and for other steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at 888-453-9048 Monday through Friday 9:00 am - 7:00 pm Eastern, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Mandy Kellogg
Administrative Services Administrator

HELENA-ADT-CM

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary 12-month membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: 11/15/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** [REDACTED]

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **11/15/2024**, and provide them engagement number [REDACTED].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**North Carolina
Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

**Washington, DC
Attorney General**
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

**City of St. Helena
Administrative Services**

1088 College Ave.
St. Helena, CA 94574
cityofsthelena.org



August 23, 2024

Notice of Data Breach

Dear :

On behalf of The City of St. Helena, I am writing to inform you of an incident involving unauthorized access to some of your information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On May 13, 2024, we detected unauthorized activity on our network. We promptly began investigating to determine the scope of the incident and working with cybersecurity experts on remediation. Once we identified the impacted data, we engaged a data-review firm to review the content of those files. We received those results on August 7, 2024, and promptly determined which individuals to notify.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that an unauthorized third party accessed materials on our network containing your personal information, including your name, contact information, date of birth, financial account details (such as a bank account or credit card number), and government identification number (such as a passport number, driver's license number, or Social Security number).

WHAT WE ARE DOING

We hired third-party experts to help us address this situation. They investigated the unauthorized activity and worked with us to further secure our systems.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity, and we are offering a complimentary 12-month membership to Experian's IdentityWorks. Please also review the next page for steps to enroll in IdentityWorks and for other steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at 888-453-9048 Monday through Friday 9:00 am - 7:00 pm Eastern, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Mandy Kellogg
Administrative Services Administrator

HELENA-ADT-CMF

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary 12-month membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: 11/15/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** [REDACTED]

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **11/15/2024**, and provide them engagement number [REDACTED].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**North Carolina
Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

**Washington, DC
Attorney General**
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

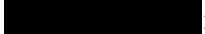
**City of St. Helena
Administrative Services**

1088 College Ave.
St. Helena, CA 94574
cityofsthelena.org



August 23, 2024

Notice of Data Breach

Dear :

On behalf of The City of St. Helena, I am writing to inform you of an incident involving unauthorized access to some of your information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On May 13, 2024, we detected unauthorized activity on our network. We promptly began investigating to determine the scope of the incident and working with cybersecurity experts on remediation. Once we identified the impacted data, we engaged a data-review firm to review the content of those files. We received those results on August 7, 2024, and promptly determined which individuals to notify.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that an unauthorized third party accessed materials on our network containing your personal information, including your name, contact information, date of birth, financial account details (such as a bank account or credit card number), government identification number (such as a passport number, driver's license number, or Social Security number), and limited medical information (such as treatment details, insurance information, or similar records we received).

WHAT WE ARE DOING

We hired third-party experts to help us address this situation. They investigated the unauthorized activity and worked with us to further secure our systems.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity, and we are offering a complimentary 12-month membership to Experian's IdentityWorks. Please also review the next page for steps to enroll in IdentityWorks and for other steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at 888-453-9048 Monday through Friday 9:00 am - 7:00 pm Eastern, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Mandy Kellogg
Administrative Services Administrator

HELENA-ADT-CMFM

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary 12-month membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: 11/15/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** [REDACTED]

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **11/15/2024**, and provide them engagement number [REDACTED].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**North Carolina
Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

**Washington, DC
Attorney General**
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

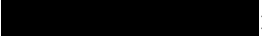
**City of St. Helena
Administrative Services**

1088 College Ave.
St. Helena, CA 94574
cityofsthelena.org



August 23, 2024

Notice of Data Breach

Dear :

On behalf of The City of St. Helena, I am writing to inform you of an incident involving unauthorized access to some of your information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On May 13, 2024, we detected unauthorized activity on our network. We promptly began investigating to determine the scope of the incident and working with cybersecurity experts on remediation. Once we identified the impacted data, we engaged a data-review firm to review the content of those files. We received those results on August 7, 2024, and promptly determined which individuals to notify.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that an unauthorized third party accessed materials on our network containing your personal information, including your name, contact information, date of birth, government identification number (such as a passport number, driver's license number, or Social Security number), and limited medical information (such as treatment details, insurance information, or similar records we received).

WHAT WE ARE DOING

We hired third-party experts to help us address this situation. They investigated the unauthorized activity and worked with us to further secure our systems.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity, and we are offering a complimentary 12-month membership to Experian's IdentityWorks. Please also review the next page for steps to enroll in IdentityWorks and for other steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at 888-453-9048 Monday through Friday 9:00 am - 7:00 pm Eastern, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Mandy Kellogg
Administrative Services Administrator

HELENA-ADT-CMM

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary 12-month membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: 11/15/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** [REDACTED]

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **11/15/2024**, and provide them engagement number [REDACTED].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**North Carolina
Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

**Washington, DC
Attorney General**
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

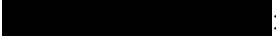
**City of St. Helena
Administrative Services**

1088 College Ave.
St. Helena, CA 94574
cityofsthelena.org



August 23, 2024

Notice of Data Breach

Dear :

On behalf of The City of St. Helena, I am writing to inform you of an incident involving unauthorized access to some of your information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On May 13, 2024, we detected unauthorized activity on our network. We promptly began investigating to determine the scope of the incident and working with cybersecurity experts on remediation. Once we identified the impacted data, we engaged a data-review firm to review the content of those files. We received those results on August 7, 2024, and promptly determined which individuals to notify.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that an unauthorized third party accessed materials on our network containing your personal information, including your name, contact information, date of birth, and financial account details (such as bank account or credit card numbers).

WHAT WE ARE DOING

We hired third-party experts to help us address this situation. They investigated the unauthorized activity and worked with us to further secure our systems.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity. Please also review the next page for steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at 888-453-9048 Monday through Friday 9:00 am - 7:00 pm Eastern, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Mandy Kellogg
Administrative Services Administrator

HELENA-ADT-F

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**North Carolina
Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

**Washington, DC
Attorney General**
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.