



Richard Goldberg, Partner & Vice-Chair
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
rgoldberg@constangy.com
Mobile: 917.744.1760

July 15, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Panoramic Financial Management ("Panoramic"), a single operator tax services business operating in Minnesota, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute Md. Code Ann. Comm. Law §§ 14-3501 - 3508

1. Nature of the Security Incident

On July 8, 2024, Panoramic identified a group of clients whose data may have been involved in a data security incident. The incident occurred in February 2024, when Panoramic became aware of unusual activity in a software used for tax preparation. Panoramic immediately took steps to secure its systems and began an investigation to determine what happened. In June the investigation resulted in a determination that an unauthorized person may have gained access to some personal information of some Panoramic clients.

Panoramic then worked diligently to ascertain the identities of involved individuals and the types of their information that may have been involved in this incident. It also worked to identify current contact information to notify individuals about this incident. This step was completed on July 8, 2024.

On July 15, 2024 Panoramic mailed notifications to all individuals identified in the investigation, providing them with steps they can take to protect their personal information, and offering free credit and identity monitoring services for adults.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for 2 Maryland residents. The information involved in the incident included the individual's Social Security number.

3. Notification to Affected Individuals

On July 15, 2024, a notification letter was sent to the affected MD residents by United States Postal Service First Class Mail. The notification letter provides resources and steps the individual can take to help protect their information. The notification letter also offers 12 months of complimentary identity protection services including credit monitoring for adults, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

Panoramic terminated the unauthorized access on its network and began an investigation into what happened. Panoramic has also instituted Panoramic has sent notices to the potentially affected individuals and is providing them with steps they can take to protect their personal information as discussed above and reporting the incident to nationwide consumer reporting agencies (i.e., Equifax, Experian, and Transunion).

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at RGoldberg@constangy.com or 917.744.1760.

Sincerely,



Richard Goldberg
Constangy, Brooks, Smith & Prophete LLP

RG:EHS

Encl.: Sample Notification Letter

cc: Ethan H. Schutzman, Constangy (eschutzman@constangy.com)

PAUL W. SWANSON CPA/PFS MBT CFP™

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 15, 2024

Notice of Data <<Incident/Breach>>

Dear <<First Name>> <<Last Name>>,

I am writing you about a data security incident that may have affected your personal information. As you know, my firm takes the privacy and security of personal information of my clients very seriously which is why I am informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services.

What Happened. On July 8, 2024, the investigation into whose information may have been involved in a cyber incident ended and we learned who to notify. The incident began on February 15, 2024, when the firm became aware of unusual activity in a software used for tax preparation and immediately took steps to secure our systems. Cybersecurity experts assisted with the process. The investigation eventually revealed that certain data may have been acquired without authorization. A secondary investigation then commenced to determine whose information may have been involved in the incident. That review concluded on July 8, 2024, and identified that some of your information may have been involved.

What Information Was Involved. The potentially affected information may have included your name, address, and Social Security number.

What We Are Doing. As soon as we discovered the incident, we took steps described above and conferred with experts regarding network security to minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and Internal Revenue Service and will provide whatever cooperation may be necessary to hold the perpetrators accountable.

In addition, we are offering identity theft protection services through IDX, a nationwide data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of 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.

What You Can Do. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-800-939-4170 going to <https://app.idx.us/account-creation/protect>, and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 am – 8:00 pm Central Time. Please note, the deadline to enroll is October 15, 2024.

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online, so please do not discard this letter.

Please call 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

I sincerely regret any anxiety or difficulty caused by this incident.

Sincerely,

Paul W. Swanson

Paul W Swanson, CPA/PFS MBT CFFP™
12504 Norway Circle
Burnsville, MN 55337

(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. 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.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 agencies 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 a 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. You can 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

PAUL W. SWANSON CPA/PFS MBT CFP™

P.O. Box 989728
West Sacramento, CA 95798-9728

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 15, 2024

Notice of Data <<Incident/Breach>>

Dear Parent or Guardian of <<First Name>> <<Last Name>>,

I am writing you about a data security incident that may have affected your child's personal information. As you know, my firm takes the privacy and security of personal information of my clients very seriously which is why I am informing you of the incident, providing you with steps you can take to protect your child's personal information, and offering your child complimentary identity protection services.

What Happened. On July 8, 2024, the investigation into whose information may have been involved in a cyber incident ended and we learned who to notify. The incident began on February 15, 2024, when the firm became aware of unusual activity in a software used for tax preparation and immediately took steps to secure our systems. Cybersecurity experts assisted with the process. The investigation eventually revealed that certain data may have been acquired without authorization. A secondary investigation then commenced to determine whose information may have been involved in the incident. That review concluded on July 8, 2024 and identified that some of your child's information may have been involved.

What Information Was Involved. The potentially affected information may have included your child's name, address, and Social Security number.

What We Are Doing. As soon as we discovered the incident, we took steps described above and conferred with experts regarding network security to minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and Internal Revenue Service and will provide whatever cooperation may be necessary to hold the perpetrators accountable.

In addition, we are offering identity theft protection services through IDX, a nationwide data breach and recovery services expert. IDX identity protection services include: <<12/24>> months CyberScan dark web monitoring, fully managed identity recovery services, and \$1 million in identity theft insurance coverage. With this protection, IDX will help you resolve issues if your child's identity is compromised.

What You Can Do. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 am – 8:00 pm Central Time. Please note, the deadline to enroll is October 15, 2024.

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online, so please do not discard this letter.

Please call 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

I sincerely regret any anxiety or difficulty caused by this incident.

Sincerely,

Paul W. Swanson

Paul W Swanson, CPA/PFS MBT CFFP™
12504 Norway Circle
Burnsville, MN 55337

(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

3. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Security Freeze. You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files.

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 agencies 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 a 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. You can 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.