PCH Digital, LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

Publishers Clearing House

[redacted]

November 5, 2026

NOTICE OF DATA BREACH

Dear [redacted],

PCH Digital is writing to inform you about a data-security event involving some of your personal information. We are providing this notice to give you information about what happened, what we are doing in response, and how you can enroll in our offer of free credit monitoring services.

What Happened?

On February 18, 2026, we detected suspicious activity in a portion of a legacy computer network. We promptly began working with third-party cybersecurity experts to investigate and remediate that activity. In April, the investigation found that an unauthorized third party gained access to a portion of our computer network from February 4 to 18, 2026. We identified the files impacted by the event, migrated data to a new environment with increased safeguards, and then engaged a data-review firm to analyze the affected files' contents. We received the data-review results in September and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

What Information Was Involved?

We determined that the impacted files contained some of your personal information, which includes your: name, contact information, and government identification number (such as a Social Security number).

What We Are Doing.

We worked with third-party experts to address this event, perform an investigation into the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement, which did not delay this notice.

What You Can Do.

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page. Additionally, to help protect you from fraud or identity theft, we are offering you a complimentary 12-month membership to TransUnion's credit monitoring and proactive fraud assistance. To enroll in those services:

- Ensure that you enroll by: **January 28, 2027** (Your code will not work after this date.)
- Visit TransUnion's website to enroll: **https://mytrueidentity.com**
- Provide your activation code: [redacted]

Recycle Me!

Please note that when signing up for these services, you may be asked to verify personal information for your own protection. We use that information to confirm your identity.

For More Information.

Should you have any questions, you can contact us at [redacted] between the hours of 8:00 a.m. and 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

PCH Digital

Recycle Me!

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. Contact your financial institution if you see errors or activity you don't recognize on your account statements. Get your free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting yourself from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave. NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

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 prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe you are the victim of fraud or identity theft, consider notifying your attorney general or the Federal Trade Commission. You also have the right to file a police report and request a copy of that report.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit:
https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect yourself from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.oag.maryland.gov.
- **New York Residents**. You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6000 or (877) 566-7226 or visit their website, www.ncdoj.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main St., Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 403 Rhode Island residents.

Recycle Me!

PCH Digital, LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

[redacted]

November 5, 2026

NOTICE OF DATA BREACH

Dear [redacted],

PCH Digital is writing to inform you about a data-security event involving some of your personal information. We are providing this notice to give you information about what happened, what we are doing in response, and what steps you can take.

What Happened?

On February 18, 2026, we detected suspicious activity in a portion of a legacy computer network. We promptly began working with third-party cybersecurity experts to investigate and remediate that activity. In April, the investigation found that an unauthorized third party gained access to a portion of our computer network from February 4 to 18, 2026. We identified the files impacted by the event, migrated data to a new environment with increased safeguards, and then engaged a data-review firm to analyze the affected files' contents. We received the data-review results in September and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

What Information Was Involved?

We determined that the impacted files contained some of your personal information, which includes your: name, contact information, and limited medical information (such as diagnoses, treatment details, or information about medical conditions that you chose to share with us).

What We Are Doing.

We worked with third-party experts to address this event, perform an investigation into the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement, which did not delay this notice.

What You Can Do.

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page.

Recycle Me!

For More Information.

Should you have any questions, you can contact us at [redacted] between the hours of 8:00 a.m. and 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

PCH Digital

Recycle Me!

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. Contact your financial institution if you see errors or activity you don't recognize on your account statements. Get your free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting yourself from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave. NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

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 prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe you are the victim of fraud or identity theft, consider notifying your attorney general or the Federal Trade Commission. You also have the right to file a police report and request a copy of that report.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit:
https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect yourself from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.oag.maryland.gov.
- **New York Residents**. You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6000 or (877) 566-7226 or visit their website, www.ncdoj.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main St., Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 403 Rhode Island residents.

Recycle Me!

PCH Digital, LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

To the Parent or Guardian of
[redacted]

November 5, 2026

NOTICE OF DATA BREACH

Dear Parent or Guardian of David Khlebnikov,

PCH Digital is writing to inform you about a data-security event involving some of your child's personal information. We are providing this notice to give you information about what happened, what we are doing in response, and how you can enroll your child in our offer of free cyber-monitoring services.

What Happened?

On February 18, 2026, we detected suspicious activity in a portion of a legacy computer network. We promptly began working with third-party cybersecurity experts to investigate and remediate that activity. In April, the investigation found that an unauthorized third party gained access to a portion of our computer network from February 4 to 18, 2026. We identified the files impacted by the event, migrated data to a new environment with increased safeguards, and then engaged a data-review firm to analyze the affected files' contents. We received the data-review results in September and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

What Information Was Involved?

We determined that the impacted files contained some of your child's personal information, which includes their: name, contact information, and government identification number (such as a Social Security number).

What We Are Doing.

We worked with third-party experts to address this event, perform an investigation into the unauthorized activity, and further secure our systems to protect your child's information. We also notified law enforcement, which did not delay this notice.

What You Can Do.

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page. Additionally, to help protect your child from fraud or identity theft, we are offering them a complimentary 12-month membership to TransUnion's cyber-monitoring services. Cyber monitoring will look out for your and your child's personal data on the dark web. If you enroll, TransUnion will alert you if your personally identifiable information or your child's information is found online. To enroll in the cyber monitoring, please:

- Ensure you enroll by: **January 28, 2027** (Your child's code will not work after this date.)

Recycle Me!

- Visit TransUnion's website to enroll: **https://bfs.cyberscout.com/activate**
- Provide the activation code: [redacted]

Please note that when signing up for these services, you may be asked to verify personal information for your protection. We use that information to confirm your identity.

For More Information.

Should you have any questions, you can contact us at [redacted] between the hours of 8:00 a.m. and 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

PCH Digital

Recycle Me!

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your child's account statements and free credit reports. Contact your child's financial institution if you see errors or activity you don't recognize on their account statements. Get your child's free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting your child from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave. NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

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

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending your child credit that they should take special precautions to verify your child's 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 child's credit report, which makes it harder for someone to open an account in their name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe your child is the victim of fraud or identity theft, consider notifying your state's attorney general or the Federal Trade Commission. You also have the right to file a police report and request a copy of that report.

Review the Fair Credit Reporting Act – Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your child's rights pursuant to the FCRA, please visit: https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect your child from fraud or identity theft.

- **Maryland Residents**. You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.oag.maryland.gov.
- **New York Residents**. You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6000 or (877) 566-7226 or visit their website, www.ncdoj.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main St., Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 403 Rhode Island residents.

Recycle Me!

PCH Digital, LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

To the Parent or Guardian of
[redacted]

November 5, 2026

NOTICE OF DATA BREACH

Dear Parent or Guardian of [redacted],

PCH Digital is writing to inform you about a data-security event involving some of your child's personal information. We are providing this notice to give you information about what happened, what we are doing in response, and what steps you can take.

What Happened?

On February 18, 2026, we detected suspicious activity in a portion of a legacy computer network. We promptly began working with third-party cybersecurity experts to investigate and remediate that activity. In April, the investigation found that an unauthorized third party gained access to a portion of our computer network from February 4 to 18, 2026. We identified the files impacted by the event, migrated data to a new environment with increased safeguards, and then engaged a data-review firm to analyze the affected files' contents. We received the data-review results in September and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

What Information Was Involved?

We determined that the impacted files contained some of your child's personal information, which includes their: name, contact information, and birthdate.

What We Are Doing.

We worked with third-party experts to address this event, perform an investigation into the unauthorized activity, and further secure our systems to protect your child's information. We also notified law enforcement, which did not delay this notice.

What You Can Do.

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page.

Recycle Me!

For More Information.

Should you have any questions, you can contact us at [redacted] between the hours of 8:00 a.m. and 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

PCH Digital

Recycle Me!

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your child's account statements and free credit reports. Contact your child's financial institution if you see errors or activity you don't recognize on their account statements. Get your child's free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting your child from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave. NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

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

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending your child credit that they should take special precautions to verify your child's 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 child's credit report, which makes it harder for someone to open an account in their name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe your child is the victim of fraud or identity theft, consider notifying your state's attorney general or the Federal Trade Commission. You also have the right to file a police report and request a copy of that report.

Review the Fair Credit Reporting Act – Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your child's rights pursuant to the FCRA, please visit:
https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect your child from fraud or identity theft.

- **Maryland Residents**. You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.oag.maryland.gov.
- **New York Residents**. You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6000 or (877) 566-7226 or visit their website, www.ncdoj.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main St., Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 403 Rhode Island residents.

Recycle Me!