SQUIRE PATTON BOGGS

Squire Patton Boggs (US) LLP
1000 Key Tower
127 Public Square
Cleveland, Ohio 44114

O +1 216 479 8500
F +1 216 479 8780
squirepattonboggs.com

November 22, 2023

VIA E-MAIL (AttorneyGeneral@doj.nh.gov)

Consumer Protection & Antitrust Bureau
Office of the Attorney General
Supreme Court Building
1 Granite Place South
Concord, NH 03301

RE: Notification of Potential Data Security Incident

Dear Attorney General Formella:

The Pinal County Superintendent's Office ("PCSO"), located at 75 N. Bailey Street, Florence, Arizona 85132, has retained Squire Patton Boggs (US) LLP ("SPB") in connection with a cybersecurity incident that may have involved the personal information of approximately two (2) New Hampshire residents. PCSO is reporting a potential cybersecurity incident that occurred on or around September 25, 2023 (the "Incident") pursuant to NH Rev. Stat. § 359-C:20(VI)(a). This notice provides details about the Incident and PCSO's response and remediation efforts. SPB will supplement this notice, as appropriate, with any new significant facts discovered subsequent to this submission. PCSO does not waive any rights or defenses relating to the incident, this notice, or the applicability of New Hampshire law on personal jurisdiction.

PCSO is an educational service agency that assists in processing payroll and other related administrative services on behalf of 23 public school districts in Pinal County, Arizona, their respective current and former employees, and such employees' dependents. On or around September 25, 2023, PCSO was locked out of the data processing environment by a suspected ransomware attack. PCSO restored its data using available and viable backups and coordinated closely with state and federal law enforcement agencies to secure its environment. PCSO also retained third-party experts, including an IT firm to conduct a thorough forensic investigation into the circumstances surrounding the Incident, and outside counsel to advise on legal obligations.

On or around November 3, 2023, PCSO's investigation determined that personal information may have been affected, including individuals'

The New Hampshire residents potentially impacted by the Incident will receive notice via U.S. Mail. An example of the notifications mailed to the affected New Hampshire residents is attached and includes complimentary credit monitoring and identity theft insurance for .

If you have any additional questions, please do not hesitate to contact me.

Sincerely,

Colin R. Jennings, Partner
Squire Patton Boggs (US) LLP

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

PINAL COUNTY

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

November 17, 2023

Dear <<First Name>>:

We are writing to share with you important information regarding a network security incident that may have potentially involved your personally identifiable information ("PII") relating to your employment with a school serviced by the Pinal County Superintendent's Office ("PCSO"). We take this incident very seriously and are providing you with information, as well as access to resources as a precaution to safeguard and protect your PII.

What Happened:

On or about September 25, 2023, PCSO experienced a network security incident, which resulted in the potential compromise of a portion of PCSO's data processing environment. PSCO processes payroll and provides other related administrative services on behalf of certain Pinal County school districts and their respective employees, including your current employer.

The incident was first discovered on September 25, 2023, when employees of PCSO were "locked out" of the PCSO data processing environment. In response, among other things, PCSO restored its data from available and viable backups and coordinated closely with state and federal law enforcement agencies to secure its environment. Further, PCSO retained an IT firm to conduct a thorough forensic investigation into the circumstances surrounding the incident.

While our investigation is still ongoing, there is no forensic evidence to confirm that your PII was compromised. **Because we are committed to protecting your personal data, we are proactively providing you this notice, in an abundance of caution, so that you may diligently monitor your accounts**.

What Information Was Involved:

The type of PII that PCSO maintains because of your employment with your local school district may include the following:

What PCSO is Doing:

The confidentiality of PII is one of PCSO's top priorities. Immediately upon learning of the incident, we took steps to contain the incident and conduct a thorough investigation. The third-party forensic and cyber security IT firm we retained also assisted in the remediation of our system, including eliminating the vulnerability that was used by the unauthorized actor and implementing additional security measures. As such, we have already strengthened our system, and will continue to do so throughout this response process and beyond.

Credit Monitoring Services:

While PCSO is not aware of any identity fraud or improper use of any PII as a direct result of this incident, out of an abundance of caution, we have arranged to have Cyberscout, a TransUnion company, provide you with twenty-four (24) months of complimentary credit monitoring services through Identity Force and identity theft insurance. To activate your membership in these services, please follow the steps outlined at the end of this letter.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

If you have any questions about this notice or the incident, please telephone the Cyberscout call center at 1-833-707-0465 from 8:00 am to 8:00 pm ET, Monday through Friday, excluding holidays, for ninety (90) days from the date of this letter.

We value you and sincerely apologize for any inconvenience caused by this incident. Thank you for your understanding.

Sincerely,

Jill Broussard
Pinal County Superintendent

Credit Monitoring Services

Activation Codes

<<First Name>> <<Last Name>> << unique code>>

In response to the network security incident, PCSO has engaged Cyberscout, a TransUnion company specializing in fraud assistance and remediation services, to provide the following services through Identity Force:

- Single Bureau Credit Monitoring, Report and Score;
- Cyber Monitoring
- Identity Protection Services
- Identity Resolution Services
- $1,000,000 in Identity Theft Insurance

These services provide you with alerts for from the date of enrollment when changes occur to your credit file. A notification will be sent to you the same day that the changes or updates takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft, as well as a $1,000,000 insurance reimbursement policy. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

How do I enroll for the free services?

To register your account and activate your services type the following URL into your browser: **https://secure.identityforce.com/benefit/pinalcounty** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<unique code>>**.

For you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your State's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one (1) free credit report annually from each of the three (3) major credit reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three (3) credit reporting agencies below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Div.	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting one of the three (3) major credit reporting agencies at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three (3) major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts ninety (90) days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. There is no cost to place a credit freeze. When a credit freeze is in place, no one— including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security Number;

3. Date of birth;

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;

5. Proof of current address, such as a current utility bill or telephone bill;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);

7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and

8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven (7) years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three (3) credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

ADDITIONAL RESOURCES

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

Your state Attorney General may also have advice on preventing identity theft and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.

Massachusetts Residents: If applicable, you have the right to obtain a police report regarding this Incident.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

Iowa Residents: The Attorney General can be contacted at 1305 E. Walnut St. Des Moines, IA 50319; (515) 281-5164; or https://www.iowaattorneygeneral.gov/.

Oregon Residents: The Attorney General can be contacted at 1162 Court St. NE Salem, OR 97301-4096; (877) 877-9392; or https://www.doj.state.or.us/.

Rhode Island Residents: The Attorney General can be contacted at 4 Howard Avenue Cranston, RI 02920; (401) 274-4400; or http://www.riag.ri.gov/index.php. You may also file or obtain any police report filed in regard to this incident.

District of Columbia Residents: The Attorney General can be contacted at Office of Attorney General, 400 6th Street, NW, Washington, DC 20001; (202) 727-3400; or https://oag.dc.gov/.

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

PINAL COUNTY

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

November 17, 2023

Dear <<First Name>>:

We are writing to share with you important information regarding a network security incident that may have potentially involved your personally identifiable information ("PII") and those of your dependent(s) (collectively, "you"), relating to your employment with a school serviced by the Pinal County Superintendent's Office ("PCSO"). Note, any affected dependent(s) are listed on page three. We take this incident very seriously and are providing you with information, as well as access to resources as a precaution to safeguard and protect your PII.

What Happened:

On or about September 25, 2023, PCSO experienced a network security incident, which resulted in the potential compromise of a portion of PCSO's data processing environment. PSCO processes payroll and provides other related administrative services on behalf of certain Pinal County school districts and their respective employees, including your current employer.

The incident was first discovered on September 25, 2023, when employees of PCSO were "locked out" of the PCSO data processing environment. In response, among other things, PCSO restored its data from available and viable backups and coordinated closely with state and federal law enforcement agencies to secure its environment. Further, PCSO retained an IT firm to conduct a thorough forensic investigation into the circumstances surrounding the incident.

While our investigation is still ongoing, there is no forensic evidence to confirm that your PII was compromised. **Because we are committed to protecting your personal data, we are proactively providing you this notice, in an abundance of caution, so that you may diligently monitor your accounts.**

What Information Was Involved:

The type of PII that PCSO maintains because of your employment with your local school district may include the following:

What PCSO is Doing:

The confidentiality of PII is one of PCSO's top priorities. Immediately upon learning of the incident, we took steps to contain the incident and conduct a thorough investigation. The third-party forensic and cyber security IT firm we retained also assisted in the remediation of our system, including eliminating the vulnerability that was used by the unauthorized actor and implementing additional security measures. As such, we have already strengthened our system, and will continue to do so throughout this response process and beyond.

Credit Monitoring Services:

While PCSO is not aware of any identity fraud or improper use of any PII as a direct result of this incident, we have arranged to have Cyberscout, a TransUnion company, provide you with twenty-four (24) months of complimentary credit monitoring services through Identity Force and identity theft insurance. To activate your membership in these services, please follow the steps outlined at the end of this letter.

In addition, if applicable, we have arranged to have your minor dependents' (*i.e.,* those dependents under 18 years of age) information monitored on the dark web. To activate your dependents' membership in these services, please follow the steps outlined at the end of this letter.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

If you have any questions about this notice or the incident, please telephone the Cyberscout call center at 1-833-707-0465 from 8:00 am to 8:00 pm ET, Monday through Friday, excluding holidays, for ninety (90) days from the date of this letter.

We value you and sincerely apologize for any inconvenience caused by this incident. Thank you for your understanding.

Sincerely,

Jill Broussard
Pinal County Superintendent

Credit Monitoring Services

Activation Codes

<<First Name>> <<Last Name>> << unique code>>

<<custom field 1 >>

<<custom field 2 >>

<<custom field 3 >>

<<custom field 4 >>

<<custom field 5>>

<<custom field 6 >>

<<custom field 7 >>

<<custom field 8>>

In response to the network security incident, PCSO has engaged Cyberscout, a TransUnion company specializing in fraud assistance and remediation services, to provide the following services through Identity Force:

- Single Bureau Credit Monitoring, Report and Score;
- Cyber Monitoring
- Identity Protection Services
- Identity Resolution Services
- $1,000,000 in Identity Theft Insurance

These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. A notification will be sent to you the same day that the changes or updates takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft, as well as a $1,000,000 insurance reimbursement policy. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

How do I enroll for the free services?

To register your account and activate your services type the following URL into your browser: **https://secure.identityforce.com/benefit/pinalcounty** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<unique code>>**.

Once you have enrolled and created your online account, you will be able to offer the services to a spouse by clicking on 'Add My Spouse'. Also, you will be able to enter your children's information for monitoring on the dark web. For you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your State's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one (1) free credit report annually from each of the three (3) major credit reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three (3) credit reporting agencies below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Div.	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting one of the three (3) major credit reporting agencies at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three (3) major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts ninety (90) days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. There is no cost to place a credit freeze. When a credit freeze is in place, no one— including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security Number;

3. Date of birth;

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;

5. Proof of current address, such as a current utility bill or telephone bill;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);

7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and

8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven (7) years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three (3) credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

ADDITIONAL RESOURCES

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

Your state Attorney General may also have advice on preventing identity theft and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.

Massachusetts Residents: If applicable, you have the right to obtain a police report regarding this Incident.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

Iowa Residents: The Attorney General can be contacted at 1305 E. Walnut St. Des Moines, IA 50319; (515) 281-5164; or https://www.iowaattorneygeneral.gov/.

Oregon Residents: The Attorney General can be contacted at 1162 Court St. NE Salem, OR 97301-4096; (877) 877-9392; or https://www.doj.state.or.us/.

Rhode Island Residents: The Attorney General can be contacted at 4 Howard Avenue Cranston, RI 02920; (401) 274-4400; or http://www.riag.ri.gov/index.php. You may also file or obtain any police report filed in regard to this incident.

District of Columbia Residents: The Attorney General can be contacted at Office of Attorney General, 400 6th Street, NW, Washington, DC 20001; (202) 727-3400; or https://oag.dc.gov/.

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

PINAL COUNTY

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

November 17, 2023

Dear <<First Name>>:

We are writing to share with you important information regarding a network security incident that may have potentially involved your personally identifiable information ("PII") relating to your former employment with a school serviced by the Pinal County Superintendent's Office ("PCSO"). We take this incident very seriously and are providing you with information, as well as access to resources as a precaution to safeguard and protect your PII.

What Happened:

On or about September 25, 2023, PCSO experienced a network security incident, which resulted in the potential compromise of a portion of PCSO's data processing environment. PSCO processes payroll and provides other related administrative services on behalf of certain Pinal County school districts and their respective employees, including your former employer.

The incident was first discovered on September 25, 2023, when employees of PCSO were "locked out" of the PCSO data processing environment. In response, among other things, PCSO restored its data from available and viable backups and coordinated closely with state and federal law enforcement agencies to secure its environment. Further, PCSO retained an IT firm to conduct a thorough forensic investigation into the circumstances surrounding the incident.

While our investigation is still ongoing, there is no forensic evidence to confirm that your PII was compromised. **Because we are committed to protecting your personal data, we are proactively providing you this notice, in an abundance of caution, so that you may diligently monitor your accounts**.

What Information Was Involved:

The type of PII that PCSO maintains because of your former employment with a local school district may include the following:

What PCSO is Doing:

The confidentiality of PII is one of PCSO's top priorities. Immediately upon learning of the incident, we took steps to contain the incident and conduct a thorough investigation. The third-party forensic and cyber security IT firm we retained also assisted in the remediation of our system, including eliminating the vulnerability that was used by the unauthorized actor and implementing additional security measures. As such, we have already strengthened our system, and will continue to do so throughout this response process and beyond.

Credit Monitoring Services:

While PCSO is not aware of any identity fraud or improper use of any PII as a direct result of this incident, out of an abundance of caution, we have arranged to have Cyberscout, a TransUnion company, provide you with of complimentary credit monitoring services through Identity Force and identity theft insurance. To activate your membership in these services, please follow the steps outlined at the end of this letter.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

If you have any questions about this notice or the incident, please telephone the Cyberscout call center at 1-833-707-0465 from 8:00 am to 8:00 pm ET, Monday through Friday, excluding holidays, for ninety (90) days from the date of this letter.

We value you and sincerely apologize for any inconvenience caused by this incident. Thank you for your understanding.

Sincerely,

Jill Broussard
Pinal County Superintendent

Credit Monitoring Services

Activation Codes

<<First Name>> <<Last Name>> << unique code>>

In response to the network security incident, PCSO has engaged Cyberscout, a TransUnion company specializing in fraud assistance and remediation services, to provide the following services through Identity Force:

- Single Bureau Credit Monitoring, Report and Score;
- Cyber Monitoring
- Identity Protection Services
- Identity Resolution Services
- $1,000,000 in Identity Theft Insurance

These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. A notification will be sent to you the same day that the changes or updates takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft, as well as a $1,000,000 insurance reimbursement policy. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

How do I enroll for the free services?

To register your account and activate your services, type the following URL into your browser: **https://secure.identityforce.com/benefit/pinalcounty** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<unique code>>**.

For you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your State's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one (1) free credit report annually from each of the three (3) major credit reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three (3) credit reporting agencies below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Div.	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting one of the three (3) major credit reporting agencies at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three (3) major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts ninety (90) days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. There is no cost to place a credit freeze. When a credit freeze is in place, no one— including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security Number;

3. Date of birth;

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;

5. Proof of current address, such as a current utility bill or telephone bill;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);

7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and

8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven (7) years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three (3) credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

ADDITIONAL RESOURCES

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

Your state Attorney General may also have advice on preventing identity theft and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.

Massachusetts Residents: If applicable, you have the right to obtain a police report regarding this Incident.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

Iowa Residents: The Attorney General can be contacted at 1305 E. Walnut St. Des Moines, IA 50319; (515) 281-5164; or https://www.iowaattorneygeneral.gov/.

Oregon Residents: The Attorney General can be contacted at 1162 Court St. NE Salem, OR 97301-4096; (877) 877-9392; or https://www.doj.state.or.us/.

Rhode Island Residents: The Attorney General can be contacted at 4 Howard Avenue Cranston, RI 02920; (401) 274-4400; or http://www.riag.ri.gov/index.php. You may also file or obtain any police report filed in regard to this incident.

District of Columbia Residents: The Attorney General can be contacted at Office of Attorney General, 400 6th Street, NW, Washington, DC 20001; (202) 727-3400; or https://oag.dc.gov/.

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

November 17, 2023

Dear <<First Name>>:

We are writing to share with you important information regarding a network security incident that may have potentially involved your personally identifiable information ("PII") and those of your dependent(s) (collectively, "you"), relating to your former employment with a school serviced by the Pinal County Superintendent's Office ("PCSO"). Note, any affected dependent(s) are listed on page three. We take this incident very seriously and are providing you with information, as well as access to resources as a precaution to safeguard and protect your PII.

What Happened:

On or about September 25, 2023, PCSO experienced a network security incident, which resulted in the potential compromise of a portion of PCSO's data processing environment. PSCO processes payroll and provides other related administrative services on behalf of certain Pinal County school districts and their respective employees, including your former employer.

The incident was first discovered on September 25, 2023, when employees of PCSO were "locked out" of the PCSO data processing environment. In response, among other things, PCSO restored its data from available and viable backups and coordinated closely with state and federal law enforcement agencies to secure its environment. Further, PCSO retained an IT firm to conduct a thorough forensic investigation into the circumstances surrounding the incident.

While our investigation is still ongoing, there is no forensic evidence to confirm that your PII was compromised. **Because we are committed to protecting your personal data, we are proactively providing you this notice, in an abundance of caution, so that you may diligently monitor your accounts.**

What Information Was Involved:

The type of PII that PCSO maintains because of your former employment with a local school district may include the following:

What PCSO is Doing:

The confidentiality of PII is one of PCSO's top priorities. Immediately upon learning of the incident, we took steps to contain the incident and conduct a thorough investigation. The third-party forensic and cyber security IT firm we retained also assisted in the remediation of our system, including eliminating the vulnerability that was used by the unauthorized actor and implementing additional security measures. As such, we have already strengthened our system, and will continue to do so throughout this response process and beyond.

Credit Monitoring Services:

While PCSO is not aware of any identity fraud or improper use of any PII as a direct result of this incident, we have arranged to have Cyberscout, a TransUnion company, provide you with
of complimentary credit monitoring services through Identity Force and identity theft insurance. To activate your membership in these services, please follow the steps outlined at the end of this letter.

In addition, if applicable, we have arranged to have your minor dependents' (*i.e.,* those dependents under 18 years of age) information monitored on the dark web. To activate your dependents' membership in these services, please follow the steps outlined at the end of this letter.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

If you have any questions about this notice or the incident, please telephone the Cyberscout call center at 1-833-707-0465 from 8:00 am to 8:00 pm ET, Monday through Friday, excluding holidays, for ninety (90) days from the date of this letter.

We value you and sincerely apologize for any inconvenience caused by this incident. Thank you for your understanding.

Sincerely,

Pinal County Superintendent

Credit Monitoring Services

Activation Codes

<<First Name>> <<Last Name>> << unique code>>

<<custom field 1 >>

<<custom field 2 >>

<<custom field 3 >>

<<custom field 4 >>

<<custom field 5>>

<<custom field 6 >>

<<custom field 7 >>

<<custom field 8>>

In response to the network security incident, PCSO has engaged Cyberscout, a TransUnion company specializing in fraud assistance and remediation services, to provide the following services through Identity Force:

- Single Bureau Credit Monitoring, Report and Score;
- Cyber Monitoring
- Identity Protection Services
- Identity Resolution Services
- $1,000,000 in Identity Theft Insurance

These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. A notification will be sent to you the same day that the changes or updates takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft, as well as a $1,000,000 insurance reimbursement policy. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

How do I enroll for the free services?

To register your account and activate your services type the following URL into your browser: **https://secure.identityforce.com/benefit/pinalcounty** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<unique code>>**.

Once you have enrolled and created your online account, you will be able to offer the services to a spouse by clicking on 'Add My Spouse'. Also, you will be able to enter your children's information for monitoring on the dark web. For you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your State's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one (1) free credit report annually from each of the three (3) major credit reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three (3) credit reporting agencies below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Div.	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting one of the three (3) major credit reporting agencies at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three (3) major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts ninety (90) days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. There is no cost to place a credit freeze. When a credit freeze is in place, no one— including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security Number;

3. Date of birth;

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;

5. Proof of current address, such as a current utility bill or telephone bill;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);

7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and

8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven (7) years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three (3) credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

ADDITIONAL RESOURCES

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

Your state Attorney General may also have advice on preventing identity theft and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.

Massachusetts Residents: If applicable, you have the right to obtain a police report regarding this Incident.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

Iowa Residents: The Attorney General can be contacted at 1305 E. Walnut St. Des Moines, IA 50319; (515) 281-5164; or https://www.iowaattorneygeneral.gov/.

Oregon Residents: The Attorney General can be contacted at 1162 Court St. NE Salem, OR 97301-4096; (877) 877-9392; or https://www.doj.state.or.us/.

Rhode Island Residents: The Attorney General can be contacted at 4 Howard Avenue Cranston, RI 02920; (401) 274-4400; or http://www.riag.ri.gov/index.php. You may also file or obtain any police report filed in regard to this incident.

District of Columbia Residents: The Attorney General can be contacted at Office of Attorney General, 400 6th Street, NW, Washington, DC 20001; (202) 727-3400; or https://oag.dc.gov/.