

Morgan Lewis

Ezra D. Church

Partner
+1.215.963.5710
ezra.church@morganlewis.com

February 29, 2024

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Breach

Dear Sir or Madame:

On behalf of **PCTEL, Inc. ("PCTEL")**, pursuant to Md. Code. Com. Law § 14-3501 *et seq.*, we are writing to notify you of a cyber incident involving 128 potential Maryland residents.

Parties Involved

PCTEL is a private company that provides wireless technology solutions. PCTEL is located at 471 Brighton Drive, Bloomingdale, IL 60108.

Nature of the Incident

On November 4, 2023, PCTEL was alerted through its third-party monitoring vendor of unauthorized login attempts to its network systems. PCTEL subsequently discovered encrypted files and a ransom note from an unauthorized threat actor. PCTEL immediately initiated efforts to secure its computer systems and, with the assistance of third-party computer specialists, launched an investigation. PCTEL also notified and cooperated with federal law enforcement.

PCTEL's investigation revealed that its systems were accessed for a limited period on November 4, 2023 and November 5, 2023 and the unauthorized group deployed ransomware throughout the PCTEL network. Currently, PCTEL has not found any indicators that the unauthorized group has returned to the PCTEL network. As a result of the investigation, PCTEL recently determined potentially sensitive information was accessed by the unauthorized group and notified affected individuals on February 29, 2024.

What Information was Involved?

After PCTEL's investigation, it determined based on the affected individual that the personal information accessed included social security number/tax identification number, date of birth, financial account number, and health insurance information for some current or former employees was affected. This includes 128 current or former Maryland residents. Currently, PCTEL is not aware of any fraud or misuse of employee information.

Response to the Incident

After learning of the incident, PCTEL promptly initiated efforts to secure its system upon discovery, notified law enforcement, and initiated an investigation to determine the nature and scope of the incident. Since

the incident, PCTEL has (i) secured the affected servers; (ii) ensured the threat actors have not returned; and (iii) implemented additional enhanced monitoring, detection, and preventative controls.

The Maryland residents were notified on February 29, 2024. A sample notification letter is attached.

Identity Theft Protection

PCTEL is providing a complimentary two-year identity monitoring services through Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. These services include credit monitoring and fraud assistance and alert. None of the notified individuals have been asked or required to waive any right of private action as a condition of accepting the credit monitoring services.

Contact Information

If you have any questions concerning this matter, please contact me on behalf of PCTEL at (215) 963-5710, or ezra.church@morganlewis.com.

Best regards,

A handwritten signature in dark ink, appearing to read "Ezra D. Church".

Ezra D. Church

Enclosure

Sample Individual Notification Letters

PCTEL, Inc.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB08536 4-1



[REDACTED]

February 29, 2024

Re: Notice of Data Breach

Dear [REDACTED]:

We are writing to inform you of a recent data security incident that PCTEL Inc. ("PCTEL") experienced that might have involved some of your personal information. This letter is being sent to provide you with additional information and to advise you of services PCTEL is offering at no charge to you to help protect your continued privacy.

It is important to note that we have no evidence at this time that your personal information has been used inappropriately or fraudulently, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done, and what you can do to address this situation.

What Happened?

On November 4, 2023, we were alerted through our third-party monitoring vendor of unauthorized login attempts to our network systems. PCTEL subsequently discovered encrypted files and a ransom note from an unauthorized threat actor. We immediately initiated efforts to secure our computer systems and, with the assistance of third-party computer specialists, launched an investigation. We also notified and cooperated with federal law enforcement.

Our investigation revealed that our systems were accessed for a limited period on November 4, 2023 and November 5, 2023 and the unauthorized group deployed ransomware throughout the PCTEL network. Currently, we have not found any indicators that the unauthorized group has returned to the PCTEL network. As a result of our investigation, we recently determined potentially sensitive information was accessed by the unauthorized group and we initiated efforts to notify you.

What Information Was Involved?

The impacted files may have included your [REDACTED]. While there is no evidence that the information has been used in an unauthorized way, we did want to make you aware of the situation out of an abundance of caution and so you can take the steps outlined below to protect yourself.

What We Are Doing

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24-months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update 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 event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How Do I Enroll?

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/pctel> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED].

In order 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 email 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.

What You Can Do

If you choose not to use these services, we strongly urge you to do the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)

P.O. Box 4500

Allen, TX 75013

www.experian.com

Equifax (1-800-525-6285)

P.O. Box 740241

Atlanta, GA 30374

www.equifax.com

TransUnion (1-800-680-7289)

P.O. Box 2000

Chester, PA 19016

www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to PCTEL.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

For More Information

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,

Sumeet Paul
Director of IT

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, 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, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

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, provide 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, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
<https://ag.ny.gov/internet/resource-center>

NYS Department of State's Division of Consumer Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You

can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services.

PCTEL, Inc.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB08536 4-1



[REDACTED]

February 29, 2024

Re: Notice of Data Security Incident

Dear [REDACTED]:

We are writing to inform you of a recent data security incident that PCTEL Inc. ("PCTEL") experienced that might have involved some of your personal information. This letter is being sent to provide you with additional information and to advise you of services PCTEL is offering at no charge to you to help protect your continued privacy.

It is important to note that we have no evidence at this time that your personal information has been used inappropriately or fraudulently, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done, and what you can do to address this situation.

What Happened?

On November 4, 2023, we were alerted through our third-party monitoring vendor of unauthorized login attempts to our network systems. PCTEL subsequently discovered encrypted files and a ransom note from an unauthorized threat actor. We immediately initiated efforts to secure our computer systems and, with the assistance of third-party computer specialists, launched an investigation. We also notified and cooperated with federal law enforcement.

Our investigation revealed that our systems were accessed for a limited period on November 4, 2023 and November 5, 2023 and the unauthorized group deployed ransomware throughout the PCTEL network. Currently, we have not found any indicators that the unauthorized group has returned to the PCTEL network. As a result of our investigation, we recently determined potentially sensitive information was accessed by the unauthorized group and we initiated efforts to notify you.

What Information Was Involved?

The impacted files may have included your [REDACTED]. While there is no evidence that the information has been used in an unauthorized way, we did want to make you aware of the situation out of an abundance of caution and so you can take the steps outlined below to protect yourself.

What We Are Doing

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24-months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update 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 event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How Do I Enroll?

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/pctel> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED].

In order 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 email 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.

What You Can Do

If you choose not to use these services, we strongly urge you to do the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)

P.O. Box 4500

Allen, TX 75013

www.experian.com

Equifax (1-800-525-6285)

P.O. Box 740241

Atlanta, GA 30374

www.equifax.com

TransUnion (1-800-680-7289)

P.O. Box 2000

Chester, PA 19016

www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to PCTEL.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

For More Information

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,

Sumeet Paul
Director of IT

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, 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, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

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, provide 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, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
<https://ag.ny.gov/internet/resource-center>

NYS Department of State's Division of Consumer Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You

can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services.