



Sarah Fulton Hutchins
Partner
t: 704.335.6639
f: 704.334.4706
sarahhutchins@parkerpoe.com

RECEIVED
JUN 10 2020
CONSUMER PROTECTION
Atlanta, GA
Charleston, SC
Charlotte, NC
Columbia, SC
Greenville, SC
Raleigh, NC
Spartanburg, SC
Washington, DC

June 5, 2020

Via FedEx

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Breach Notification

To Whom It May Concern

My firm represents DAK Americas LLC, a global manufacturing company headquartered in Charlotte, North Carolina.

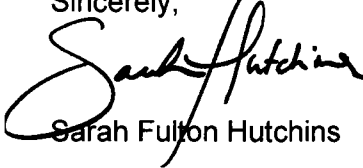
On December 16, 2019, a malicious program was inadvertently installed on a legacy server. It remained passive until March 14, 2020, when it began installing encryption software on certain networks. Late in the evening on March 15, 2020, the attackers began encrypting folders on the server. The attack has been designated a ransomware attack. Within 24 hours, DAK Americas isolated and shut down the infected systems. After coordinating with law enforcement and working with an independent cybersecurity company, there is no indication that data was removed from the affected systems.

In response to the attack, DAK Americas worked with law enforcement, an independent cybersecurity company, and a law firm. It has offered the services described in the attached letters to all affected persons, all of whom were either current or former employees. DAK Americas has also followed the recommendations of the cybersecurity firm to increase security, including but not limited to increased password security requirements for administrative accounts, eliminating certain domain mailboxes to minimize opportunities for attacks, deploying next generation endpoint protections on all systems, isolating legacy system, initiating dark web monitoring, and increasing restrictions on remote access to corporate servers.

Attached are the two template notifications being sent to affected persons in New Hampshire. Those notifications will be sent through U.S. Mail by the end of the week (June 5, 2020). Please direct any follow-up inquiries to Sarah Hutchins, sarahhutchins@parkerpoe.com, 704.372.9000.

PPAB 5655835v1

Consumer Protection Bureau
June 5, 2020
Page 2

Sincerely,

Sarah Fulton Hutchins

SFH:ad
Attachments

June 2, 2020

1 1 329 *****AUTO**MIXED AADC 300

John Doe
123 Anystreet Dr
Anytown, NY 12345



Re: Notice of Data Breach

Dear John Doe,

DAK Americas is writing to notify you of a recent data security incident that may have exposed some of your personal information. While there is currently no evidence that your information has been misused as a result of this incident, we are providing you with information about the incident, our response to it, and information related to what you may do to better protect your personal information, should you feel it appropriate to do so.

What Happened? On March 15, 2020, we became aware of unusual activity relating to certain corporate systems. We identified the attack and within 24 hours had contained the breach. We immediately began an investigation with the assistance of third-party vendors and law enforcement to help us close off the improper access and assess the impact of any potential data breach. The investigation determined that a certain legacy virtual server was accessed without authorization and infected with ransomware. It is possible that over 3,000 individuals' personal information may have been affected by the incident, which includes current and former employees. Based on the results of an independent digital forensics team, we do not believe that personal information was viewed or removed by the unauthorized actor, but out of an abundance of caution we immediately began a thorough review of the contents of the server to determine whether sensitive information was present at the time of the incident.

What Information was Involved? Our investigation determined that at the time of the incident the infected server contained information including employees' names, driver's license or state identification numbers, Social Security numbers, and salary information.

What Are We Doing. Information, privacy, and security are among our highest priorities. DAK Americas has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to investigate and confirm the security of our systems, and in an abundance of caution we quickly disabled access to the affected server. We hired a cybersecurity firm to conduct a global investigation into how the incident occurred and assist our team with understanding the scope of the impact. We also engaged Parker Poe, a law firm we work with, and cooperated with law enforcement officials who also investigated the incident.

We believe we have cut off the threat. As part of our ongoing commitment to the security of information, we implemented increased security measures, conducted additional employee training, initiated dark web monitoring,

and are currently reviewing our policies and procedures relating to data security. Additionally, we are also providing relevant regulatory notices.

While, to date, we have no evidence of actual or attempted misuse of your information as a result of this incident, we are notifying you so that you may take further steps to better protect your personal information should you feel it is appropriate to do so. We secured the services of NortonLifeLock, Inc. to provide identity and credit monitoring services at no cost to you for twenty-four (24) months. For more information on these services, please review the enclosed "Steps You Can Take to Protect Your Information."

What Can You Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity for the next twelve (12) to twenty-four (24) months. To take advantage of this monitoring, you must enroll. You may review the information contained in the attached "Steps You Can Take to Protect Your Information." You may enroll in LifeLock Defender Preferred™ to receive the identity and credit monitoring services we are making available to you as we are unable to enroll in these services on your behalf.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at (866) 775-2037 (toll free), available 24/7.

DAK Americas takes the privacy and security of the personal information in our care seriously. Please let us know if you have any questions.

Sincerely

N. Eammon G. Simmons

N. Eammon G. Simmons
Senior Director – Human Resources
DAK Americas LLC

Steps You Can Take to Protect Your Information

Complimentary Credit Monitoring and Identity Protection Services

DAK Americas has retained NortonLifeLock, Inc. to provide twenty-four (24) months of complimentary **LifeLock Defender™ Preferred** identity theft protection.

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to www.LifeLock.com. Click on the yellow "START MEMBERSHIP" button (do not attempt registration from a link presented by a search engine).
2. You will be taken to another page where, below the FOUR protection plan boxes, you may enter the **Promo Code:** [REDACTED] and click the "APPLY" button.
3. On the next screen, enter your **Member ID:** [REDACTED] and click the "APPLY" button.
4. Your complimentary offer is presented. Click the red "START YOUR MEMBERSHIP" button.
5. Once enrollment is completed, you will receive a confirmation email (be sure to follow ALL directions in this email).

Alternatively, to activate your membership over the phone, please call: (866) 775-2037.

You will have until July 31st, 2020 to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your LifeLock Defender™ Preferred membership includes:

- ✓ Primary Identity Alert System[†]
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring^{**}
- ✓ Norton™ Security Deluxe² (90 Day Free Subscription)
- ✓ Stolen Funds Reimbursement up to \$25,000^{†††}
- ✓ Personal Expense Compensation up to \$25,000^{†††}
- ✓ Coverage for Lawyers and Experts up to \$1 million^{†††}
- ✓ U.S.-based Identity Restoration Team
- ✓ Annual Three-Bureau Credit Reports & Credit Scores^{1**}
The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.
- ✓ Three-Bureau Credit Monitoring^{1**}
- ✓ USPS Address Change Verification Notifications
- ✓ Fictitious Identity Monitoring
- ✓ Credit, Checking and Savings Account Activity Alerts^{†**}

¹Your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.

No one can prevent all identity theft or cybercrime.

² Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.

[†] LifeLock does not monitor all transactions at all businesses.

^{**}These features are not enabled upon enrollment. Member must take action to get their protection.

^{†††} Reimbursement and Expense Compensation, each with limits of up to \$25,000 for Defender Preferred. And up to \$1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To

order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

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 a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or www.oag.state.md.us.

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

For Iowa residents: you are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, <https://www.iowaattorneygeneral.gov/for-consumers>, 1-888-777-4590.

June 2, 2020

3 1 504 *****AUTO**ALL FOR AADC 294

John Doe

123 Anystreet Dr

Anytown, NY 12345



Re: Notice of Data Breach

Dear John Doe,

DAK Americas is writing to notify you of a recent data security incident that may have exposed some of your personal information. While there is currently no evidence that your information has been misused as a result of this incident, we are providing you with information about the incident, our response to it, and information related to what you may do to better protect your personal information, should you feel it appropriate to do so.

What Happened? On March 15, 2020, we became aware of unusual activity relating to certain corporate systems. We identified the attack and within 24 hours had contained the breach. We immediately began an investigation with the assistance of third-party vendors and law enforcement to help us close off the improper access and assess the impact of any potential data breach. The investigation determined that a certain legacy virtual server was accessed without authorization and infected with ransomware. It is possible that over 3,000 individuals' personal information may have been affected by the incident, which includes current and former employees. Based on the results of an independent digital forensics team, we do not believe that personal information was viewed or removed by the unauthorized actor, but out of an abundance of caution, we immediately began a thorough review of the contents of the server to determine whether sensitive information was present at the time of the incident.

What Information was Involved? Our investigation determined that at the time of the incident the infected server contained information including employees' names, driver's license or state identification numbers, Social Security numbers, and salary information.

What Are We Doing. Information, privacy, and security are among our highest priorities. DAK Americas has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to investigate and confirm the security of our systems, and in an abundance of caution we quickly disabled access to the affected server. We hired a cybersecurity firm to conduct a global investigation into how the incident occurred and assist our team with understanding the scope of the impact. We also engaged Parker Poe, a law firm we work with, and cooperated with law enforcement officials who also investigated the incident.

We believe we have cut off the threat. As part of our ongoing commitment to the security of information, we implemented increased security measures, conducted additional employee training, initiated dark web monitoring, and are currently reviewing our policies and procedures relating to data security. Additionally, we are also providing relevant regulatory notices.

While, to date, we have no evidence of actual or attempted misuse of your information as a result of this incident, we are notifying you so that you may take further steps to better protect your personal information should you feel it is appropriate to do so. We would like to remind you that one of your employee benefits is access to LifeLock Identity Theft Protection. For more information on these services, please review the enclosed "Steps You Can Take to Protect Your Information."

What Can You Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity for the next twelve (12) to twenty-four (24) months. You may review the information contained in the attached "Steps You Can Take to Protect Your Information." Make sure you are enrolled in LifeLock Identity Theft Protection to receive the identity and credit monitoring services we have made available to you as we are unable to enroll in these services on your behalf.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, you may contact Cheryl R. Hoskins, Senior Corporate Benefits Representative for DAK Americas either by email (Cheryl.hoskins@alpekpolyester.com) or phone (704-940-7562).

DAK Americas takes the privacy and security of the personal information in our care seriously. Please let us know if you have any questions.

Sincerely,

N. Eammon G. Simmons

N. Eammon G. Simmons
Senior Director – Human Resources
DAK Americas LLC

Steps You Can Take to Protect Your Information

LifeLock Identity Theft Plans

You were already offered LifeLock Identity Theft Protection through our benefit offering! LifeLock's proprietary technology can detect a wide range of identity threats[†] and if there's a problem, a dedicated, U.S.-based Identity Restoration Specialist will personally handle your case from start to finish and help fix it. This service includes free credit and identity monitoring services. It's all backed by our Million Dollar Protection™ Package^{††}, to help you keep what's yours, yours.

If you would like to update your current LifeLock election, please login to the HR, Benefits & Pay Portal at <https://workforcenow.adp.com> today to enroll.

No one can prevent all identity theft.

† LifeLock does not monitor all transactions at all businesses.

††† Reimbursement and Expense Compensation, each with limits of up to \$1 million for Benefit Elite and Ultimate Plus and up to \$25,000 for Junior. And up to \$1 million for coverage for lawyers and experts if needed, for all plans. Benefits provided by Master Policy issued by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

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 a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or www.oag.state.md.us.

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

For Iowa residents: you are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, <https://www.iowaattorneygeneral.gov/for-consumers>, 1-888-777-4590