

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

March 17, 2022

Sent via Online Submission

Office of the Attorney General
6 State House Station
Augusta, ME 04333

Dear Attorney General Aaron Frey,

We represent Allied Benefit Systems, LLC (“Allied”) as outside counsel with respect to a data security incident involving personal information as described below. Allied, headquartered in Illinois, is notifying you on behalf of its business customer, who is the owner of the impacted data. (See Enclosure A).

1. Nature of security incident.

On January 21, 2021, Allied identified suspicious activity associated with one of its corporate email accounts. Allied immediately began an investigation, revoked all multi-factor authentication sessions, and changed the password to the account. Allied’s investigation determined that an unauthorized user gained access to the account on January 21, 2021, established a forwarding rule to send responses to an internal folder, and sent spam emails from the account. The unauthorized access lasted for less than forty-five (45) minutes, and there was no synching or downloading of the contents of the account. Given the short period of time that the unauthorized actor had access to the email account and the activities taken by the individual while present in the account, Allied believes it is highly unlikely that any sensitive information was accessed or acquired. However, Allied is a licensed entity in New York, and the New York Department of Financial Services (“NYDFS”) requested that Allied review and extract any personal information contained in the account. Allied subsequently engaged a vendor to assist with this process, and recently received the output file as a result of this process. Allied then took steps to ensure data owners were notified of the incident and offered to mail letters to impacted individuals on behalf of the data owners.

2. Number of residents affected.

Three (3) Maine residents may have been affected and were notified of the incident. For those that requested Allied mail letters, a letter was sent to the potentially affected individuals on March 17, 2022 via regular mail (a copy of the form notification letter is enclosed). Impacted information

may include name, date of birth, Social Security number, and health benefits and enrollment information.

3. Steps taken in response to the incident.

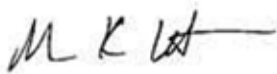
Since this incident, Allied changed the user's password, revoked all MFA sessions, and retrained the employee on recognizing and responding to suspicious computer activity. Additionally, impacted individuals were offered months of credit monitoring and identity protection services through Kroll.

4. Contact information.

Allied takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 651-4616.

Sincerely,

CLARK HILL



Melissa K. Ventrone
Member

cc: Mariah Leffingwell – mleffingwell@clarkhill.com

Enclosure A

Company Name	Total
Douglas Products & Packaging LLC	3



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA SECURITY INCIDENT

Dear <<first_name>> <<last_name>>,

Allied Benefit Systems, LLC (“Allied”) experienced a data security incident that may have impacted your personal information. Allied is a third-party claims processor for group health plans, and may have obtained your personal information from your employer or previous employer <<b2b_text_1(Employer)>> for the purpose of potentially providing administrative services for your employer’s group health plan. Allied takes the privacy and security of your information seriously, and sincerely apologizes for any concern or inconvenience this may cause you. While we believe there is no risk that any of your information has been or will be misused, we want to provide you with details regarding this incident, and resources we are making available to help you.

What happened?

On January 21, 2021, Allied identified suspicious activity associated with one of its corporate email accounts. Allied immediately began an investigation, revoked all multi-factor authentication (“MFA”) sessions, and changed the password to the account. Allied’s investigation determined that an unauthorized user gained access to the account on January 21, 2021, established a forwarding rule to send responses to an internal folder, and sent spam emails from the account. The unauthorized access lasted for less than forty-five (45) minutes, and there was no syncing or downloading of the contents of the account. Given the short period of time that the unauthorized actor had access to the email account and the activities taken by the individual while present in the account, we believe it highly unlikely that any sensitive information was accessed or acquired. However, out of an abundance of caution, we retained a third party to identify any personal information that may have been contained in the account.

What Information Was Involved?

On November 8, 2021, we learned that your <<b2b_text_2(DataElements)>> may have been in the account at the time of the incident.

What we are doing:

Although we do not believe there is any risk that your information will be misused, we have secured the services of Kroll to provide identity monitoring at no cost to you for **12** months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(EnrollmentDeadline)>> to activate your identity monitoring services.

Membership Number: <<MembershipNumber(S_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Additional information describing your services is included with this letter.

Additionally, in response to this incident Allied changed the employee's password, revoked all MFA sessions, and retrained the employee on recognizing and responding to suspicious computer activity.

What you can do:

While we believe there is no risk that your information has been or will be misused, it is always a good idea to remain vigilant for incidents of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information:

If you have any questions or concerns, please call 1-855-618-1657 Monday through Friday from 8:00 am – 5:30 pm Central Time, excluding major US holidays. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Allied Benefit Systems, LLC

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

You've been provided with access to the following services from Kroll:

1. Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data-for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

2. Fraud Consultation. You have unlimited access to consultation with a Kroll specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

3. Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

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

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

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

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

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

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

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

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

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

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

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

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

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident.

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



<<Date>> (Format: Month Day, Year)

The Parent or Guardian of

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_3(NOTICE OF DATA SECURITY INCIDENT / NOTICE OF DATA BREACH - CA only)>>

The Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Allied Benefit Systems, LLC (“Allied”) experienced a data security incident that may have impacted your minor or dependent’s personal information. Allied is a third-party claims processor for group health plans, and may have obtained your minor or dependent’s personal information from your employer or previous employer, Douglas Products & Packaging, for the purpose of potentially providing administrative services for your employer’s group health plan. Allied takes the privacy and security of this information seriously, and sincerely apologizes for any concern or inconvenience this may cause you. While we believe there is no risk that any of this information has been or will be misused, we want to provide you with details regarding this incident, and resources we are making available to help you.

What happened?

On January 21, 2021, Allied identified suspicious activity associated with one of its corporate email accounts. Allied immediately began an investigation, revoked all multi-factor authentication (“MFA”) sessions, and changed the password to the account. Allied’s investigation determined that an unauthorized user gained access to the account on January 21, 2021, established a forwarding rule to send responses to an internal folder, and sent spam emails from the account. The unauthorized access lasted for less than forty-five (45) minutes, and there was no synching or downloading of the contents of the account. Given the short period of time that the unauthorized actor had access to the email account and the activities taken by the individual while present in the account, we believe it highly unlikely that any sensitive information was accessed or acquired. However, out of an abundance of caution, we retained a third party to identify any personal information that may have been contained in the account.

What Information Was Involved?

On November 8, 2021, we learned that your minor or dependent’s <<b2b_text_2(Name, DataElements)>> may have been in the account at the time of the incident.

What we are doing:

In response to this incident, Allied changed the employee’s password, revoked all MFA sessions, and retrained the employee on recognizing and responding to suspicious computer activity. To request to enroll in minor identity monitoring, call the toll free number below¹. You will need to provide the call center with the following reference number: <<Membership Number s_n>>.

What you can do:

While we believe there is no risk that your minor or dependent’s information has been or will be misused, it is always a good idea to remain vigilant for incidents of identity theft or fraud, and to review any available statements for suspicious activity. Additional information about protecting your minor or dependent’s identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze.

¹Credit monitoring is not available for minors.

For More Information:

If you have any questions or concerns, please call (855) 618-1657 Monday through Friday from 8:00 am – 5:30 pm Central Time, excluding major U.S. holidays. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Allied Benefit Systems, LLC

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

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

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

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

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351

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

Experian Fraud Reporting and Credit Freeze
P.O. Box 9554
Allen, TX 75013

1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289

www.transunion.com

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

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

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

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

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

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident.

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