MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Matthew V. Toldero
Office: (267) 930-4554
Fax: (267) 930-4771
Email: mtoldero@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 2, 2021

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent OperationsInc LLC ("OperationsInc"), located at 383 Main Avenue, 4th Floor, Norwalk, CT 06851, and we are writing on behalf of its impacted data owner clients, COFCO Americas Resources Corp. and International Cotton Depots, Inc., to notify your office of an incident that may affect the privacy of certain personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned after its submission. By providing this notice, OperationsInc does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 21, 2021, OperationsInc received a report of suspicious email activity that occurred in August 2017 and resulted in the transfer of information related to certain COFCO Americas Resources Corp. and International Cotton Depots, Inc. employees from an OperationsInc employee to an unauthorized individual via email. The transfer occurred in response to a phishing email, which was sent by the unauthorized individual to the OperationsInc employee and purported to be from an OperationsInc executive. Believing the email to be legitimate, the OperationsInc employee sent the requested information in response, which included certain individuals' names and Social Security numbers. OperationsInc cannot confirm if the unauthorized person(s) accessed or viewed any specific information relating to individuals.

Upon learning of this incident, OperationsInc worked quickly and diligently to validate the activity reported. OperationsInc recently learned that individuals associated with COFCO Americas Resources Corp. and International Cotton Depots, Inc were potentially impacted and provided notice of this conclusion to COFCO Americas Resources Corp. and International Cotton Depots, Inc on July 12, 2021. OperationsInc then worked with COFCO Americas Resources Corp. and International Cotton Depots, Inc to provide direct notice to the individuals identified and put resources in place to assist them.

Notice to New Hampshire Resident

On or about September 2, 2021, OperationsInc provided written notice of this incident to potentially impacted individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter included herein as ***Exhibit A***.

Other Steps Taken and To Be Taken

OperationsInc is committed to protecting the confidentiality, privacy, and security of the information it collects in providing services to its clients and their employees. As such, OperationsInc has taken steps to enhance email security, including by disabling legacy authentication protocols and increasing workforce training on the topics of data privacy and vigilance to social engineering schemes.

As an added precaution, OperationsInc is also providing potentially impacted individuals with complimentary access to 24 months of credit monitoring and identity restoration services through Kroll, along with guidance on how to better protect against the possibility of information misuse.

Additionally, OperationsInc is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. OperationsInc is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4554.

Very truly yours,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/eyl

EXHIBIT A

OperationsInc
HUMAN RESOURCES CONSULTING

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

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

NOTICE OF <<b2b_text_1(RE: Line)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

OperationsInc is writing to inform you of an email phishing event that may impact the privacy of some of your information. OperationsInc provides human resources consulting services to <<b2b_text_2(Data Owner Name)>>. We obtained your information through our provision of such services. We are providing you with details about the event, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On June 21, 2021, we received a report of suspicious email activity that occurred in August 2017 and resulted in the transfer of information related to certain <<b2b_text_2(Data Owner Name)>> employees from an OperationsInc employee to an unauthorized individual via email. The transfer occurred in response to a phishing email, which was sent by the unauthorized individual to the OperationsInc employee and purported to be from an OperationsInc executive. Believing the email to be legitimate, the OperationsInc employee sent the requested information in response, which included your name and Social Security number. Upon learning of this incident, we worked quickly and diligently to validate the activity reported and provide this notice.

What Information Was Involved? We cannot confirm if the unauthorized person(s) accessed or viewed any specific information relating to you. However, we determined that the information transferred included your name and Social Security number.

What We Are Doing. We are committed to protecting the confidentiality, privacy, and security of the information we collect in providing services to our clients and their employees. As such, we have taken steps to enhance email security, including by disabling legacy authentication protocols and increasing workforce training on the topics of data privacy and vigilance to social engineering schemes.

As an added precaution, we are also providing you with access to 24 months of complimentary identity monitoring services through Kroll, along with guidance on how to better protect against the possibility of information misuse. We are covering the cost of these services, but due to privacy restrictions, you will need to complete the activation process yourself using the instructions below.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanations of benefits, as applicable, and by monitoring your free credit reports for suspicious activity and to detect errors. You can find out more about how to better protect against the potential misuse of information in the enclosed *Steps You Can Take to Help Protect Information.* There, you will also find more information about the monitoring services we are offering and how to activate these services.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call (855) 545-2013, 9:00 a.m. to 6:30 p.m. Eastern Time, excluding some U.S. holidays. You may also write to us at: OperationsInc LLC, ATTN: Angela McDermott, 383 Main Avenue, Fourth Floor, Norwalk, CT 06851-4866.

We apologize for any inconvenience this event may cause you and remain committed to the privacy of information in our possession.

Sincerely,

A. McDermott

Angela McDermott
Chief Operating Officer
OperationsInc

Steps You Can Take to Help Protect Information

Activate Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 24 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 **November 15, 2021** to activate your identity monitoring services.*

Membership Number: <<Membership Number s_n>>

Additional information describing your services is included with this letter.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

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 will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud 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.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Matthew V. Toldero
Office: (267) 930-4554
Fax: (267) 930-4771
Email: mtoldero@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 2, 2021

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent OperationsInc LLC ("OperationsInc") located at 383 Main Avenue, 4th Floor, Norwalk, CT 06851, and are writing to notify your office of an incident that may affect the privacy of certain personal information relating to four (4) New Hampshire residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned after its submission. By providing this notice, OperationsInc does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about May 28, 2021, OperationsInc received a report of suspicious email activity that may have been related to an employee's email account. OperationsInc promptly commenced an investigation to determine the nature and scope of the activity. The investigation determined that an email phishing campaign targeted the OperationsInc employee's email account and resulted in unauthorized person(s) briefly logging into the account on March 31, 2021. However, the investigation was unable to determine which, if any, emails and attachments in the account were viewed by the unauthorized person(s). Out of an abundance of caution, OperationsInc undertook a thorough review of the account's contents to determine whether they contained any sensitive information. On July 1, 2021, OperationsInc completed this review and determined that information related to certain individuals associated Atlas Holdings LLC ("Atlas Holdings"), a client of OperationsInc, was present in the email account during the relevant time period. Specifically, OperationsInc determined that the following information related to New Hampshire

residents was present in the account and therefore accessible: name, mailing address, Social Security number, health insurer company name, health insurance member ID number, birth date, hire date, effective date of health insurance, medical plan ID, and gender. OperationsInc provided notice of this determination to Atlas Holdings on July 12, 2021. OperationsInc then worked with Atlas Holdings to provide direct notice to the individuals identified and put resources in place to assist them.

Notice to New Hampshire Residents

On or about September 2, 2021, OperationsInc provided written notice of this incident to affected individuals, which includes four (4) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

OperationsInc is committed to protecting the confidentiality, privacy, and security of the information it collects in providing services to its clients. As such, OperationsInc has taken steps to enhance email security, including by rotating account credentials, disabling legacy authentication protocols, and increasing workforce training on the topics of data privacy and vigilance to social engineering schemes.

As an added precaution, OperationsInc is also providing potentially impacted individuals with complimentary access to 24 months of credit monitoring and identity restoration services through Kroll, along with guidance on how to better protect against the possibility of information misuse.

Additionally, OperationsInc is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. OperationsInc is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4554.

Very truly yours,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/eyl

EXHIBIT A

OperationsInc
HUMAN RESOURCES CONSULTING

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

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

NOTICE OF <<b2b_text_1(RE: Line)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

OperationsInc is writing to inform you of a recent event that may impact the privacy of some of your information. OperationsInc provides certain consulting services to Atlas Holdings LLC. We obtained your information through our provision of such services. Although we are unaware of any actual or attempted misuse of your information, we are providing you with details about the event, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On or about May 28, 2021, we received a report of suspicious email activity that may have been related to an OperationsInc employee's email account. We promptly commenced an investigation to determine the nature and scope of the activity. The investigation determined that an email phishing campaign targeted the employee's email account and resulted in unauthorized person(s) briefly logging into the account on March 31, 2021. However, the investigation was unable to determine which, if any, emails and attachments in the account were viewed by the unauthorized person(s). Out of an abundance of caution, we undertook a thorough review of the account's contents to determine whether they contained any sensitive information. On or about July 1, 2021, we determined that information related to you was present in the email account during the relevant time period.

What Information Was Involved? We cannot confirm if the unauthorized person(s) accessed or viewed any specific information relating to you. However, we determined that the information present in the relevant account included your <<b2b_text_2(Data Elements)>>.

What We Are Doing. Information privacy and security are among our highest priorities. We promptly rotated the employee's email account password and have taken further steps to enhance the security of our computer systems. As part of our ongoing commitment to the privacy and security of information in our care, we are providing enhanced training to our broader employee base on the how to detect suspicious emails. We are in the process of reviewing our existing policies and procedures to better prevent future events.

As an added precaution, we are also providing you with access to 24 months of identity monitoring services through Kroll, along with guidance on how to better protect against the possibility of information misuse. We are covering the cost of these services, but due to privacy restrictions, you will need to complete the activation process yourself using the instructions below.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanations of benefits, as applicable, and by monitoring your free credit reports for suspicious activity and to detect errors. You can find out more about how to better protect against the potential misuse of information in the enclosed *Steps You Can Take to Help Protect Information.* There, you will also find more information about the identity monitoring services we are offering and how to activate these services.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call 1-???-???-????, 9:00 a.m. to 6:30 p.m. Eastern Time, excluding some U.S. holidays. You may also write to us at: OperationsInc LLC, ATTN: Angela McDermott, 383 Main Avenue, Fourth Floor, Norwalk, CT 06851-4866.

We apologize for any inconvenience this event may cause you and remain committed to the privacy of information in our possession.

Sincerely,

Angela McDermott
Chief Operating Officer
OperationsInc

Steps You Can Take to Help Protect Information

Activate Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. 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 **December 10, 2021** to activate your identity monitoring services.*

Membership Number: <<Membership Number s_n>>

Additional information describing your services is included with this letter.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are five Rhode Island residents impacted by this incident.

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

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

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 will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud 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.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.