



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

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

August 11, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Hub International Limited (“HUB”) located at 150 N Riverside Plaza, Chicago, IL 60606, and are writing to notify your office of an event that may affect information relating to five thousand eight hundred fifty-nine (5,859) Maryland residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, HUB does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 17, 2023, HUB identified suspicious activity on certain systems within its network. In response, HUB promptly isolated the impacted systems and commenced a forensic investigation. The investigation determined that certain systems within the network were accessed by an unknown individual and files were copied without authorization between December 2022 and January 2023. HUB is in the midst of a comprehensive review of the files to determine their content and to whom they relate and is providing relevant notices as information becomes available. On July 27, 2023, HUB completed its initial review and determined that the information that could have been subject to unauthorized access related to Maryland residents includes name, Social Security number, driver’s license number, financial account information, and health insurance information.

Notice to Maryland Residents

On August 11, 2023, HUB began providing written notice of this event to five thousand eight hundred fifty-nine (5,859) Maryland 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

Upon discovering the event, HUB investigated and responded, assessed the security of its systems, and worked to identify potentially impacted individuals as quickly as possible. HUB is also evaluating policies, procedures, and technical security measures and implementing additional safeguards as appropriate to further secure the information in its systems.

HUB is providing access to credit monitoring services for twelve (12) months, through Equifax, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, HUB is providing impacted individuals with guidance on how to better protect against identity theft and fraud. HUB is providing individuals with information on how to place a fraud alert and security freeze a 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.

HUB is providing written notice of this event to state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. HUB also posted notice of this event on its website and is notifying prominent media throughout the United States. Further, HUB reported this event to law enforcement.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/prs
Enclosure

EXHIBIT A



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Mail ID>>
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>
<<Country>>

August 11, 2023

<<Variable Data 1>>

Dear <<Name 1>>:

Hub International Limited (“HUB”) is writing to inform you of an event that may involve some of your information that HUB obtained in connection with the services HUB provides you. This letter provides you with information about the event, our response, and steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened? On January 17, 2023, HUB identified suspicious activity on certain systems within our network. We promptly isolated the impacted systems and commenced a forensic investigation. The investigation determined that certain systems within the network were accessed by an unknown individual and files were copied without authorization between December 2022 and January 2023. We are in the midst of a comprehensive review of the files to determine their content and to whom they relate and are providing relevant notices as information becomes available. On July 27, 2023, we completed our initial review and began the notification process.

What Information Was Involved? The following types of information about you were identified in the reviewed files: <<Data Elements>>.

What We Are Doing. We responded to this event promptly by activating our incident response plan and taking proactive measures to secure our systems and commence a comprehensive investigation. We are also evaluating policies, procedures, and technical security measures and implementing additional safeguards as appropriate to further secure the information in our systems. We reported this event to law enforcement and relevant regulators. We are notifying and working with our affected business partner customers to provide notice to potentially impacted individuals.

As an added precaution, HUB is offering you access to <<CM Duration>> of complimentary credit monitoring and identity theft protection services. You will find information on how to enroll in these complimentary services in the “Steps You Can Take to Protect Information” section of this letter. We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. We also recommend you review the information in the “Steps You Can Take to Protect Personal Information” section of this letter.

For More Information. If you have questions about this matter, please contact our dedicated assistance line at 833-627-2764, Monday through Friday from 9:00 a.m. to 9:00 p.m. EST, (excluding holidays). You may also visit our dedicated website at www.hubinternational.com/supportinquiries/.

Sincerely,

Hub International Limited

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services



<<NAME 1>>

Enter your Activation Code: <<ACTIVATION CODE>>

Enrollment Deadline: <<ENROLLMENT DEADLINE>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. You may write to HUB at or Attn: HUB Data Event Team, 150 N Riverside Plaza, Chicago, IL 60606.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_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.

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>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Kevin M. Mekler
Office: (267) 930-2190
Fax: (267) 930-4771
Email: Kmekler@mullen.law

3001 N. Rocky Point Drive East, Suite 200
Tampa, FL 33607

April 16, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Hub International Limited located at 150 N Riverside Plaza, Chicago, IL 60606. We are supplementing HUB's previous notice to your office on August 11, 2023, and any subsequent updates thereto. By providing this notice, HUB does not waive any rights or defenses regarding personal jurisdiction or the applicability of Maryland law, including the Maryland data breach notification statute and/or potentially applicable insurance laws and regulations. By way of this supplemental notice, HUB is sharing confidential commercial and financial information. Should there be a request to share any information regarding this event beyond your Office, we ask that you advise us of the same in advance of any disclosure. Disclosure of such information could harm or impair HUB's private interest in controlling the availability of intrinsically valuable records, including records relating to security and business operations.

The investigation into this matter is now complete, and we are providing a final update regarding the number of Maryland residents potentially affected by this event. As detailed in our prior notice to your office, on August 11, 2023, HUB began providing written notice of this event to five thousand eighty hundred fifty-nine (5,859) Maryland residents. Subsequently, as information became available, HUB provided additional written notice of this event to a total of two hundred eighty-seven (287) Maryland residents on September 28, 2023, February 9, 2024, March 22, 2024, and April 12, 2024. The information that could have been subject to unauthorized access related to these additional residents includes name, Social Security number, financial account information, medical information, and health insurance information.

Should you have any additional questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2190.

Very truly yours,

Kevin M. Mekler of
MULLEN COUGHLIN LLC

KMM/prs