

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

March 17, 2022

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Hufcor Holdings, LLC ("Hufcor") located at 2101 Kennedy Road, Janesville, Wisconsin 53545 and write to inform you of a recent data security incident.

On February 21, 2022, Hufcor was victimized by a sophisticated ransomware attack that impacted its network. Upon discovery, Hufcor immediately took steps to secure the network and began an internal investigation. Further, Hufcor engaged third-party specialists to assist with a thorough, forensic investigation. On March 2, 2022, the investigation confirmed unauthorized access to the Hufcor network from November 4, 2021 through February 2, 2022. The investigation further determined that certain Hufcor data may have been subject to unauthorized access. Hufcor then immediately reviewed its internal files and compiled a list of individuals potentially impacted and worked to obtain sufficient address information in order to provide notification.

On March 4, 2022, the review was completed and it was determined that information related to 11 Maryland residents was potentially subject to unauthorized access. While the investigation into the full nature and scope of this incident remains ongoing, the information believed to be at risk includes current and former employee names, in combination with human resources related information, such as Social Security numbers and financial account information that was utilized for direct deposit purposes.

On March 17, 2022, Hufcor sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

Please contact me should you have any questions.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Meghan Farally". The signature is fluid and cursive, with the first name "Meghan" and last name "Farally" clearly distinguishable.

Meghan Farally, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A

Hufcor Holdings, LLC

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: <<XXXXXXXX>>

<<First_Name>> <<Middle_Name>> <<Last_Name>> <<Suffix>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Postal_Code>>

<<Country>>

March 17, 2022

Dear <<First_Name>> <<Middle_Name>> <<Last_Name>> <<Suffix>>:

We are writing to inform you of a cyber incident experienced by Hufcor Holdings, LLC ("Hufcor") that may have involved your information described below. While we have no evidence of attempted or actual misuse of your information as a result of this incident, we are providing you with information about the incident, our response, and steps you can take to help protect your information.

What Happened:

On February 21, 2022, Hufcor was victimized by a sophisticated ransomware attack that impacted our network. Upon discovery, we immediately began working with our I.T. team and third-party computer specialists to conduct an investigation to determine how this incident occurred. While our investigation remains ongoing, we have discovered that certain Hufcor data may have been subject to unauthorized access. Although we are unable to confirm the specific information that may be affected at this time, we are providing you with notification in an abundance of caution as we believe current and former employee information may have been impacted.

What Information Was Involved:

While our investigation into the full nature and scope of this incident remains ongoing, the information believed to be at risk includes your name, in combination with human resources related information, such as your Social Security number and financial account information that was utilized for direct deposit purposes.

What We Are Doing:

Upon discovery, we immediately engaged third-party forensic specialists to investigate this matter. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, an online credit monitoring service for 12 months provided by IDX. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can enroll to receive the complimentary credit monitoring service we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information:

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at 1-800-939-4170, Monday through Friday from 8 am – 8 pm Central Time.

We take the privacy and security of the information in our care seriously, and sincerely regret any worry or inconvenience it may cause you and your family.

Sincerely,

Kenneth Schappert

Kenneth Schappert
VP of Human Resources

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

Visit <https://app.idx.us/account-creation/protect> to activate and take advantage of your identity monitoring services.

You have until **June 17, 2022** to activate your identity monitoring services.

Enrollment Code: <<**Enrollment Code**>>

IDX Identity include the following service components:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
--	--	---

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

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.

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

January 18, 2023

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Hufcor Holdings, Inc. ("Hufcor") located at 2101 Kennedy Road, Janesville, Wisconsin 53545 and write to supplement the prior notification provided on March 17, 2022. By providing this notice, Hufcor does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On February 21, 2022, Hufcor was victimized by a sophisticated ransomware attack that impacted its network. Upon discovery, Hufcor immediately took steps to secure the network and began an internal investigation. Further, Hufcor engaged third-party specialists to assist with a thorough, forensic investigation. On March 2, 2022, the investigation confirmed unauthorized access to the Hufcor network from November 4, 2021 through February 2, 2022. The investigation further determined that certain Hufcor data may have been subject to unauthorized access, including information related to current and former employees. As a result, together with third-party specialists, Hufcor undertook a comprehensive review process in order to identify what information was potentially contained within the impacted files, and to whom that information belonged.

On March 4, 2022, the initial review related to current and former employee data was completed. On March 17, 2022, while the investigation was still ongoing, Hufcor sent written notice of this incident to potentially impacted current and former employees. There were 11 Maryland residents present in this initial population.

At the same time, the larger review of all potentially impacted files continued. This process was completed on August 23, 2022. At that time, it was determined that information related to 121 additional Maryland residents was potentially subject to unauthorized access. The information believed to potentially be at risk includes a first and last name, in combination with a Social Security number, driver's license number, financial account information, debit/credit card number, health insurance information, and/or medical information.

Prior to the completion of the review process, in June of 2022, Hufcor gave an assignment for the benefit of its creditors and entered into receivership. Due to its receivership status, Hufcor was unable to proceed with the same procedures used

to procure vendors for the initial round of notifications. Coordination with vendors and insurers became protracted, however, once the appropriate assistance was in place in December 2022, Hufcor moved quickly to provide notice to those potentially affected.

On January 13, 2023, Hufcor sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

Please contact me should you have any questions.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Meghan Farally", is written over the typed name.

Meghan Farally, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A



P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

(833) 758-9600

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

January 13, 2023

<<NOTICE OF DATA BREACH>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a cyber incident experienced by Hufcor Holdings, Inc. (“Hufcor”) that may have involved your information described below. While we have no evidence of attempted or actual misuse of your information as a result of this incident, we are providing you with information about the incident, our response, and steps you can take to help protect your information.

What Happened: On February 21, 2022, Hufcor was victimized by a sophisticated ransomware attack that impacted our network. Upon discovery, we immediately began working with our I.T. team and third-party computer specialists to conduct a full forensic investigation. We also reported this incident to federal law enforcement. Through the investigation, it was determined that certain Hufcor files may have been subject to unauthorized access. As a result, together with third-party specialists, we undertook a comprehensive review process in order to identify what information was potentially contained within the impacted files, and to whom that information belonged. That process was completed on August 23, 2022. We are now notifying those individuals whose information was potentially impacted by the incident.

What Information Was Involved: The information believed to potentially be at risk includes your first and last name, in combination with your <<Data Elements>>.

What We Are Doing: Upon discovery, we immediately engaged third-party forensic specialists to investigate this matter. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, an online credit monitoring service for <<12/24>> months provided by IDX. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do: We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can enroll to receive the complimentary credit monitoring service we are making available to you. You can also review the enclosed “Steps You Can Take to Help Protect Your Information” for additional resources.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at (833) 758-9600, Monday through Friday, from 6 a.m. to 6 p.m. Pacific Time.

We take the privacy and security of the information in our care seriously, and sincerely regret any worry or inconvenience this incident may cause you and your family.

Sincerely,

Kenneth Schappert

Kenneth Schappert
VP of Human Resources

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is April 13, 2023.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 758-9600 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); 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:

TransUnion 1-800-680-7289 www.transunion.com	Experian 1-888-397-3742 www.experian.com	Equifax 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Hufcor Holdings, Inc. may be contacted at 2101 Kennedy Road, Janesville, Wisconsin 53545.

For 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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.