

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

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

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

August 2, 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 Arpin International Group, Inc. ("AIG"), located at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893, and write to inform you of a data security incident. By providing this notice, AIG does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around April 14, 2023, AIG discovered that it was victimized by a sophisticated ransomware attack. Upon discovery, AIG immediately began working with its I.T. team and third-party forensic specialists to investigate the full nature and scope of the incident. AIG also reported this incident to federal law enforcement. While the investigation was still ongoing, it was determined that certain AIG files containing information related to AIG employees may have been subject to unauthorized access as part of the attack. AIG provided notice to potentially impacted employees on June 5, 2023. There were no Maryland residents present in the initial employee population.

Further investigation revealed a larger data set of AIG files that may have been subject to unauthorized access. As a result, AIG, with the assistance of third-party specialists, undertook a comprehensive and time-intensive process to identify the information that may have been contained within the potentially impacted files, and to whom that information belonged.

The review process revealed additional impacted data used by AIG to provide moving and relocation services for individuals, as well as various corporate clients and government agencies. AIG was in possession of this information in the normal course of business. The review of this supplementary data was completed on July 28, 2023. At that time, it was determined that information related to 1 Maryland resident was potentially subject to unauthorized access. The information believed to be at risk includes first name and last name, in combination with a date of birth and passport number.

On August 2, 2023, AIG provided written notice of this incident to the potentially impacted Maryland resident pursuant to Maryland 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,



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

Exhibit A

Return Address:
PO Box 1306
East Greenwich, RI 02818



<<First_Name>> <<Middle_Name>> <<Last_Name>> <<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Postal_Code>>
<<Country>>

August 2, 2023

<<NOTICE OF DATA BREACH>>

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

Arpin International Group, Inc. ("AIG") provides moving and relocation services for individuals, as well as various corporate clients and government agencies, including <<company name>>. AIG is providing notice of a cyber incident that we experienced that may affect the security of your information as described below. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On April 14, 2023, we discovered that we were victimized by a sophisticated ransomware attack. Upon discovery, we immediately began working with our I.T. team and third-party computer specialists to investigate the full nature and scope of the incident. We also reported this incident to federal law enforcement. Through the investigation, it was determined that certain AIG files may have been subject to unauthorized access. As a result, together with third-party specialists, we undertook a time consuming and comprehensive review process in order to identify what information was potentially contained within the impacted files, and to whom that information belonged. This process was completed on July 28, 2023. 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 and identity monitoring service for <<12/24>> months provided by IDX, a ZeroFox Company. 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 cyberincident@arpinintl.com. You may also write to us at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893.

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,

A handwritten signature in black ink, appearing to read "Peter Arpin", followed by a horizontal line.

Peter Arpin
Vice President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Out of an abundance of caution, we have arranged for you to activate identity theft protection services through IDX, a ZeroFox Company. The deadline to enroll in these services is November 1, 2023. Your unique Enrollment Code is <<enrollment code>>.

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code above.

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 **1-800-939-4170** 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 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; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Arpin International Group, Inc. may be contacted at 99 James P. Murphy Hwy, West Warwick, RI 02893.

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.

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

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

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

August 9, 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 Arpin International Group, Inc. ("AIG"), located at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893, and write to supplement the notice provided to this office on August 2, 2023. By providing this notice, AIG does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around April 14, 2023, AIG discovered that it was victimized by a sophisticated ransomware attack. Upon discovery, AIG immediately began working with its I.T. team and third-party forensic specialists to investigate the full nature and scope of the incident. AIG also reported this incident to federal law enforcement. While the investigation was still ongoing, it was determined that certain AIG files containing information related to AIG employees may have been subject to unauthorized access as part of the attack. AIG provided notice to potentially impacted employees on June 5, 2023. There were no Maryland residents present in the initial employee population.

Further investigation revealed a larger data set of AIG files that may have been subject to unauthorized access. As a result, AIG, with the assistance of third-party specialists, undertook a comprehensive and time-intensive process to identify the information that may have been contained within the potentially impacted files, and to whom that information belonged.

The review process revealed additional impacted data used by AIG to provide moving and relocation services for individuals, as well as various corporate clients and government agencies. AIG was in possession of this information in the normal course of business.

The review of data related to certain corporate clients was completed prior to the review and supplementation of the larger data set. In order to expedite notice to individuals associated with these corporate clients, written notice is being provided on a rolling basis as each client population is complete. The first round of notice to individuals associated with these corporate clients was sent on August 2, 2023. There was 1 Maryland resident present in this population.

The review process related to the next set of corporate clients was completed on August 2, 2023. At that time, it was determined that information related to 2 additional Maryland residents was potentially subject to unauthorized access. The information believed to be at risk includes first name and last name, in combination with a date of birth and passport number.

On August 8, 2023, AIG provided written notice of this incident to the additional potentially impacted Maryland residents pursuant to Maryland 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.

The review of the entire data set related to various corporate clients and government agencies remains ongoing. We will supplement this notice should additional Maryland residents be discovered in the population.

Please contact me should you have any questions.

Very truly yours,

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

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

Exhibit A

Return Address:
PO Box 1306
East Greenwich, RI 02818



<<First_Name>> <<Middle_Name>> <<Last_Name>> <<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Postal_Code>>
<<Country>>

August 8, 2023

NOTICE OF DATA BREACH

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

Arpin International Group, Inc. ("AIG") provides moving and relocation services for individuals, as well as various corporate clients and government agencies, including <<company name>>. AIG is providing notice of a cyber incident that we experienced that may affect the security of your information as described below. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On April 14, 2023, we discovered that we were victimized by a sophisticated ransomware attack. Upon discovery, we immediately began working with our I.T. team and third-party computer specialists to investigate the full nature and scope of the incident. We also reported this incident to federal law enforcement. Through the investigation, it was determined that certain AIG files may have been subject to unauthorized access. As a result, together with third-party specialists, we undertook a time consuming and comprehensive review process in order to identify what information was potentially contained within the impacted files, and to whom that information belonged. This process was completed on August 2, 2023. 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 and identity monitoring service for <<12/24>> months provided by IDX, a ZeroFox Company. 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 cyberincident@arpinintl.com. You may also write to us at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893.

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,

A handwritten signature in black ink, appearing to read "Peter Arpin".

Peter Arpin
Vice President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Out of an abundance of caution, we have arranged for you to activate identity theft protection services through IDX, a ZeroFox Company. The deadline to enroll in these services is December 7, 2023. Your unique Enrollment Code is <<enrollment code>>.

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code above.

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 **1-800-939-4170** 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag@dc.gov. Arpin International Group, Inc. may be contacted at 99 James P. Murphy Hwy, West Warwick, RI 02893.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Arpin International Group, Inc. may be contacted at 99 James P. Murphy Hwy, West Warwick, RI 02893.

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.

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

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

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

September 5, 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 Arpin International Group, Inc. ("AIG"), located at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893, and write to supplement the notices provided to this office on August 2, 2023, and August 9, 2023. By providing this notice, AIG does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around April 14, 2023, AIG discovered that it was victimized by a sophisticated ransomware attack. Upon discovery, AIG immediately began working with its I.T. team and third-party forensic specialists to investigate the full nature and scope of the incident. AIG also reported this incident to federal law enforcement. While the investigation was still ongoing, it was determined that certain AIG files containing information related to AIG employees may have been subject to unauthorized access as part of the attack. AIG provided notice to potentially impacted employees on June 5, 2023. There were no Maryland residents present in the initial employee population.

Further investigation revealed a larger data set of AIG files that may have been subject to unauthorized access. As a result, AIG, with the assistance of third-party specialists, undertook a comprehensive and time-intensive process to identify the information that may have been contained within the potentially impacted files, and to whom that information belonged.

The review process revealed additional impacted data used by AIG to provide moving and relocation services for individuals, as well as various corporate clients and government agencies. AIG was in possession of this information in the normal course of business.

The review of data related to certain corporate clients was completed prior to the review and supplementation of the larger data set. In order to expedite notice to individuals associated with these corporate clients, written notice is being provided on a rolling basis as each client population is complete. The first round of notice to individuals associated with these corporate clients was sent on August 2, 2023. There was 1 Maryland resident present in this population.

The second round of notice to individuals associated with these corporate clients was sent on August 8, 2023. There were 2 additional Maryland residents present in this population.

The review process related to the next set of corporate clients was completed on August 10, 2023. At that time, it was determined that information related to 1 additional Maryland resident was potentially subject to unauthorized access. The information believed to be at risk includes first name and last name, in combination with a passport number.

On September 1, 2023, AIG provided written notice of this incident to the additional potentially impacted Maryland residents pursuant to Maryland 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.

The review of the entire data set related to various corporate clients and government agencies was also completed on or around August 10, 2023. However, AIG is waiting on requisite approvals from impacted government agencies in order to proceed with notifying the remaining potentially impacted individuals. We will supplement this notice should additional Maryland residents be discovered in final population.

Please contact me should you have any questions.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Meghan Farally", is positioned above the printed name.

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

Exhibit A

Return Address:
PO Box 1306
East Greenwich, RI 02818



<<First_Name>> <<Middle_Name>> <<Last_Name>> <<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Postal_Code>>
<<Country>>

September 5, 2023

NOTICE OF DATA BREACH

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

Arpin International Group, Inc. ("AIG") provides moving and relocation services for individuals, as well as various corporate clients and government agencies, including <<company name>>. AIG is providing notice of a cyber incident that we experienced that may affect the security of your information as described below. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On April 14, 2023, we discovered that we were victimized by a sophisticated ransomware attack. Upon discovery, we immediately began working with our I.T. team and third-party computer specialists to investigate the full nature and scope of the incident. We also reported this incident to federal law enforcement. Through the investigation, it was determined that certain AIG files may have been subject to unauthorized access. As a result, together with third-party specialists, we undertook a time consuming and comprehensive review process in order to identify what information was potentially contained within the impacted files, and to whom that information belonged. This process was completed on August 10, 2023. 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 and identity monitoring service for <<12/24>> months provided by IDX, a ZeroFox Company. 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 cyberincident@arpinintl.com. You may also write to us at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893.

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,

A handwritten signature in black ink, appearing to read "Peter Arpin".

Peter Arpin
Vice President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Out of an abundance of caution, we have arranged for you to activate identity theft protection services through IDX, a ZeroFox Company. The deadline to enroll in these services is December 29, 2023. Your unique Enrollment Code is <<enrollment code>>.

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code above.

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 **1-800-939-4170** 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-442-9828; and oag@dc.gov. Arpin International Group, Inc. may be contacted at 99 James P. Murphy Hwy, West Warwick, RI 02893.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Arpin International Group, Inc. may be contacted at 99 James P. Murphy Hwy, West Warwick, RI 02893.

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, the consumer reporting bureaus 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 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. We encourage you to review your 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.

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

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

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

October 2, 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 Arpin International Group, Inc. ("AIG"), located at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893, and write to supplement the notices provided to this office on August 2, 2023, August 9, 2023, and September 5, 2023. By providing this notice, AIG does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around April 14, 2023, AIG discovered that it was victimized by a sophisticated ransomware attack. Upon discovery, AIG immediately began working with its I.T. team and third-party forensic specialists to investigate the full nature and scope of the incident. AIG also reported this incident to federal law enforcement. While the investigation was still ongoing, it was determined that certain AIG files containing information related to AIG employees may have been subject to unauthorized access as part of the attack. AIG provided notice to potentially impacted employees on June 5, 2023. There were no Maryland residents present in the initial employee population.

Further investigation revealed a larger data set of AIG files that may have been subject to unauthorized access. As a result, AIG, with the assistance of third-party specialists, undertook a comprehensive and time-intensive process to identify the information that may have been contained within the potentially impacted files, and to whom that information belonged.

The review process revealed additional impacted data used by AIG to provide moving and relocation services for individuals, as well as various corporate clients and government agencies. AIG was in possession of this information in the normal course of business.

The review of data related to certain corporate clients was completed prior to the review and supplementation of the larger data set. In order to expedite notice to individuals associated with these corporate clients, written notice was provided on a rolling basis as each client population was complete. The first round of notice to individuals associated with these corporate clients was sent on August 2, 2023. There was 1 Maryland resident present in this population.

The second round of notice to individuals associated with these corporate clients was sent on August 8, 2023. There were 2 additional Maryland residents present in this population.

The third round of notice to individuals associated with these corporate clients was sent on September 1, 2023. There was 1 additional Maryland resident present in this population.

The review of the entire data set related to various corporate clients and government agencies was completed on or around August 10, 2023. However, AIG needed to obtain approvals from impacted government agencies in order to proceed with notifying the remaining potentially impacted individuals. The requisite approvals were received on September 8, 2023.

There are 343 additional Maryland residents in this final population of individuals whose information was potentially subject to unauthorized access. The information believed to be at risk includes first name and last name, in combination with a Social Security number, driver's license number and/or passport number.

On September 18, 2023, AIG began providing written notice of this incident to the additional potentially impacted Maryland residents pursuant to Maryland law. The notifications were completed on September 29, 2023. The notice letter sent to individuals 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 positioned above the printed name.

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

Exhibit A



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

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

<<b2b_text_2(NOTICE OF DATA BREACH)>>

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

Arpin International Group, Inc. (“AIG”) provides moving and relocation services for individuals, as well as various corporate clients and government agencies. AIG is providing notice of a cyber incident that we experienced that may affect the security of your information as described below. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On April 14, 2023, we discovered that we were victimized by a sophisticated ransomware attack. Upon discovery, we immediately began working with our I.T. team and third-party computer specialists to investigate the full nature and scope of the incident. We also reported this incident to federal law enforcement. Through the investigation, it was determined that certain AIG files may have been subject to unauthorized access. As a result, together with third-party specialists, we undertook a time consuming and comprehensive review process in order to identify what information was potentially contained within the impacted files, and to whom that information belonged. This process was completed on August 10, 2023. 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 <<b2b_text_1(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 and identity monitoring service for 12 months provided by Kroll. 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: If you have questions, please call (866) 731-3086, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. You may also write to us at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893.

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,

A handwritten signature in black ink, appearing to read "Peter Arpin", followed by a horizontal line.

Peter Arpin
Vice President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

Visit <https://enroll.krollmonitoring.com>¹ to activate and take advantage of your identity monitoring services.

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

Membership Number: <<Membership Number s_n>>

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.

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;

¹Kroll’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.

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 Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001, 202-442-9828, and <https://oag.dc.gov/consumer-protection>. Arpin International Group, Inc. may be contacted at 99 James P. Murphy Hwy, West Warwick, RI 02893

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Arpin International Group, Inc. may be contacted at 99 James P. Murphy Hwy, West Warwick, RI 02893.

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, the consumer reporting bureaus 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 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. We encourage you to review your 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, you have the right to obtain any police report filed in regard to this incident. There are [X] Rhode Island residents impacted by this incident.

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

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

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

May 6, 2024

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 Arpin International Group, Inc. ("AIG"), located at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893, and write to supplement the prior notifications provided to this office on August 2, 2023, August 10, 2023, September 5, 2023, and October 2, 2023. By providing this notice, AIG does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On April 14, 2023, AIG discovered that it was victimized by a sophisticated ransomware attack. Upon discovery, AIG immediately began working with its I.T. team and third-party computer specialists to investigate the full nature and scope of the incident. AIG also reported this incident to federal law enforcement. Through the investigation, it was determined that certain AIG files may have been subject to unauthorized access. As a result, together with third-party specialists, AIG undertook a time consuming and comprehensive review process in order to identify what information was potentially contained within the impacted files, and to whom that information belonged. As the review progressed and AIG learned whose information may be at risk, AIG began notifying potentially impacted individuals in the summer of 2023. There was a total of 347 Maryland residents notified of this incident between June 5, 2023 and September 29, 2023.

However, in November of 2023, AIG became aware that an additional data set not previously reviewed may have also been subject to unauthorized access during the attack. AIG then began a comprehensive review of the additional impacted files, as well as a time-consuming manual review of its internal records in order to locate address information for those potentially impacted.

This thorough review process was completed on March 26, 2024. At this time, it was discovered that information related to an additional 22 Maryland residents may have been subject to unauthorized access. The information believed to be at risk for Maryland residents includes first name and last name, in combination with a Social Security number, driver's license number and/or passport number.

On May 3, 2024, AIG provided written notice of this incident to the additional potentially impacted Maryland residents pursuant to Maryland law. The notice letter sent to individuals 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,



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

Exhibit A



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

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

<<b2b_text_1 (NOTICE OF DATA BREACH)>>

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

Arpin International Group, Inc. (“AIG”) provides moving and relocation services for individuals, as well as various corporate clients and government agencies. AIG is providing notice of a cyber incident that we experienced that may affect the security of your information as described below. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On April 14, 2023, we discovered that we were victimized by a sophisticated ransomware attack. Upon discovery, we immediately began working with our I.T. team and third-party computer specialists to investigate the full nature and scope of the incident. We also reported this incident to federal law enforcement. Through the investigation, it was determined that certain AIG files may have been subject to unauthorized access. As a result, together with third-party specialists, we undertook a time consuming and comprehensive review process in order to identify what information was potentially contained within the impacted files, and to whom that information belonged. As the review progressed and we learned whose information may be at risk, we began notifying potentially impacted individuals in the summer of 2023. However, in November of 2023, we became aware that an additional data set not previously reviewed may have also been subject to unauthorized access during the attack. We then began a comprehensive review of the additional impacted files, as well as a time-consuming manual review of our internal records in order to locate address information for those potentially impacted. This thorough review process was completed on March 26, 2024. We are now notifying those individuals whose information was discovered in the secondary data set.

What Information Was Involved: The information believed to potentially be at risk includes your first and last name, in combination with your <<b2b_text_2 (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 identity monitoring service for 12 months provided by Kroll. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary identity 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 activate to receive the complimentary identity 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 [\[call center information\]](#), between 8:00 am and 5:30 pm CT, excluding major US holidays. You may also write to us at 99 James P. Murphy Highway, West Warwick, Rhode Island 02893.

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,

A handwritten signature in black ink, appearing to read "Peter Arpin", with a horizontal line extending to the right.

Peter Arpin
Vice President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

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

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

Membership Number: <<Membership Number s_n>>

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

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 will 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.

You can sign up for the online or offline identity monitoring service anytime between now and <<b2b_text_6 (activation date)>>. Due to privacy laws, we cannot register you directly. Activating in this service will not affect your credit score.

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 Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001, 202-442-9828, and <https://oag.dc.gov/consumer-protection>. Arpin International Group, Inc. may be contacted at 99 James P. Murphy Hwy, West Warwick, RI 02893.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Arpin International Group, Inc. may be contacted at 99 James P. Murphy Hwy, West Warwick, RI 02893.

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, the consumer reporting bureaus 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 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. We encourage you to review your 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, you have the right to obtain any police report filed in regard to this incident. [There are \[#\] Rhode Island residents impacted by this incident.](#)