

McAlvain Companies, Inc.  
c/o Cyberscout  
1 Keystone Ave, Unit 700  
Cherry Hill, NJ 08003  
DB08618C 1-1



April 4, 2024

*Via First-Class Mail*

**Notice of Data Security Incident**

Dear [REDACTED],

McAlvain Companies, Inc. (“MCI”) recently experienced a data security incident that may have affected your personal information. As of now we have no indication that your personal information has been or will be used inappropriately. We nevertheless wanted to make you aware of the incident and the measures we have taken in response, as well as provide details on the steps you can take – should you deem it appropriate – to help protect your information. The protection and proper use of your information is a top priority for us, and we are working to prevent a similar incident from occurring again in the future.

**What Happened**

MCI recently experienced a data security incident in which an unauthorized third party compromised MCI’s computer system. We immediately activated our incident response plan, engaged additional third-party experts, and commenced an investigation. These specialized third parties have secured our environment, hardened and enhanced our network security, and are completing a digital forensic investigation to determine how this happened as well as the extent of unauthorized activity within MCI’s network. Unfortunately, these types of incidents are becoming increasingly common and even organizations with the most sophisticated IT infrastructure available are affected. We have worked diligently to determine what happened and what information was involved as a result of this incident.

**What Information Was Involved**

Our investigation is ongoing, however it initially appears that certain human resource information may have been available for unauthorized access. The elements of your personal information that might have been impacted include: name, address, Social Security number, and date of birth. Please note that we have no evidence at this time that any of your personal information has been misused as a result of the incident.

**What We Are Doing**

We are taking this incident seriously and are committed to strengthening our systems’ security to prevent a similar event from occurring in the future. We are also focused on enhancing our cyber preparedness through additional training and updating procedures. Additionally, out of an abundance of caution, we have arranged for you to activate, at no cost to you, Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a

victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Additional information is found below.

### **What You Can Do**

To enroll in the complimentary services we are offering you, please follow the instructions provided below. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. You can enroll by using enrollment code [REDACTED] and visiting [bfs.cyberscout.com/activate](https://bfs.cyberscout.com/activate).

Please note that to activate monitoring services, you will need an internet connection and e-mail account. Additionally, you may be required to provide your name, date of birth, and Social Security number to confirm your identity. Due to privacy laws, we cannot register you directly. Please note that certain services might not be available for individuals who do not have a credit file with the credit bureaus or an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

At this time, we are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following pages, which contain important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

### **For More Information**

Please know that the protection of your personal information is a top priority, and we understand the inconvenience and concern this incident may cause. Representatives can be reached at 1-833-919-8748 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, and are available for ninety (90) days from the date of this letter to assist you with questions regarding this incident.

Sincerely,



Torry McAlvain, Jr.  
President  
McAlvain Companies, Inc.

### **Additional Important Information**

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are located below.

**Monitoring:** You should always remain vigilant and monitor your accounts for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for suspicious or unusual activity.

**Security Freeze:** You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

#### **Equifax Security Freeze**

P.O. Box 105788  
Atlanta, GA 30348  
[equifax.com/personal/credit-report-services/](https://equifax.com/personal/credit-report-services/)  
1-800-349-9960

#### **Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[experian.com/freeze/center.html](https://experian.com/freeze/center.html)  
1-888-397-3742

#### **TransUnion Security Freeze**

P.O. Box 160  
Woodlyn, PA 19094  
[transunion.com/credit-freeze](https://transunion.com/credit-freeze)  
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed below.

---

### **Implementing an Identity Protection PIN (IP PIN) with the IRS:**

To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.
- 

**For residents of Illinois, Maryland, Missouri, and North Carolina:** You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a

free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

---

**For residents of *Vermont*:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

---

**For Residents of *Washington, D.C.*:** You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov).

---

**For residents of *Maryland, Illinois, New York, and North Carolina*:** You can obtain information from your state's Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

---

**Maryland Office of the Attorney General** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 [www.oag.state.md.us](http://www.oag.state.md.us)

---

**North Carolina Office of the Attorney General** Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 [www.ncdoj.com](http://www.ncdoj.com)

---

**New York Office of Attorney General** Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

---

**Federal Trade Commission** Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

McAlvain Companies, Inc.  
c/o Cyberscout  
1 Keystone Ave, Unit 700  
Cherry Hill, NJ 08003  
DB08618C 1-1



Gordon Samson  
3014 S Ohio Ave  
Caldwell, ID 83605-5955



April 4, 2024

*Via First-Class Mail*

**Notice of Data Security Incident**

Dear Gordon Samson,

McAlvain Companies, Inc. (“MCI”) recently experienced a data security incident that may have affected your personal information. As of now we have no indication that your personal information has been or will be used inappropriately. We nevertheless wanted to make you aware of the incident and the measures we have taken in response, as well as provide details on the steps you can take – should you deem it appropriate – to help protect your information. The protection and proper use of your information is a top priority for us, and we are working to prevent a similar incident from occurring again in the future.

**What Happened**

MCI recently experienced a data security incident in which an unauthorized third party compromised MCI’s computer system. We immediately activated our incident response plan, engaged additional third-party experts, and commenced an investigation. These specialized third parties have secured our environment, hardened and enhanced our network security, and are completing a digital forensic investigation to determine how this happened as well as the extent of unauthorized activity within MCI’s network. Unfortunately, these types of incidents are becoming increasingly common and even organizations with the most sophisticated IT infrastructure available are affected. We have worked diligently to determine what happened and what information was involved as a result of this incident.

**What Information Was Involved**

Our investigation is ongoing, however it initially appears that certain human resource information may have been available for unauthorized access. The elements of your personal information that might have been impacted include: name, address, Social Security number, and date of birth. Please note that we have no evidence at this time that any of your personal information has been misused as a result of the incident.

**What We Are Doing**

We are taking this incident seriously and are committed to strengthening our systems’ security to prevent a similar event from occurring in the future. We are also focused on enhancing our cyber preparedness through additional training and updating procedures. Additionally, out of an abundance of caution, we have arranged for you to activate, at no cost to you, Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a

victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Additional information is found below.

### **What You Can Do**

To enroll in the complimentary services we are offering you, please follow the instructions provided below. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. You can enroll by using enrollment code **MCACIBFS2724** and visiting **[bfs.cyberscout.com/activate](https://bfs.cyberscout.com/activate)**.

Please note that to activate monitoring services, you will need an internet connection and e-mail account. Additionally, you may be required to provide your name, date of birth, and Social Security number to confirm your identity. Due to privacy laws, we cannot register you directly. Please note that certain services might not be available for individuals who do not have a credit file with the credit bureaus or an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

At this time, we are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following pages, which contain important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

### **For More Information**

Please know that the protection of your personal information is a top priority, and we understand the inconvenience and concern this incident may cause. Representatives can be reached at 1-833-919-8748 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, and are available for ninety (90) days from the date of this letter to assist you with questions regarding this incident.

Sincerely,

A handwritten signature in black ink, appearing to read 'Torry McAlvain, Jr.', with a stylized flourish at the end.

Torry McAlvain, Jr.  
President  
McAlvain Companies, Inc.

### **Additional Important Information**

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are located below.

**Monitoring:** You should always remain vigilant and monitor your accounts for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for suspicious or unusual activity.

**Security Freeze:** You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

**Equifax Security Freeze**

P.O. Box 105788  
Atlanta, GA 30348  
[equifax.com/personal/credit-report-services/](https://equifax.com/personal/credit-report-services/)  
1-800-349-9960

**Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[experian.com/freeze/center.html](https://experian.com/freeze/center.html)  
1-888-397-3742

**TransUnion Security Freeze**

P.O. Box 160  
Woodlyn, PA 19094  
[transunion.com/credit-freeze](https://transunion.com/credit-freeze)  
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed below.

---

### **Implementing an Identity Protection PIN (IP PIN) with the IRS:**

To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.
- 

**For residents of Illinois, Maryland, Missouri, and North Carolina:** You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a

free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

---

**For residents of *Vermont*:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

---

**For Residents of *Washington, D.C.*:** You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov).

---

**For residents of *Maryland, Illinois, New York, and North Carolina*:** You can obtain information from your state's Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

---

**Maryland Office of the Attorney General** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 [www.oag.state.md.us](http://www.oag.state.md.us)

---

**North Carolina Office of the Attorney General** Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 [www.ncdoj.com](http://www.ncdoj.com)

---

**New York Office of Attorney General** Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

---

**Federal Trade Commission** Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)