



May 31, 2024

BY EMAIL

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

To Whom It May Concern:

Form I-9 Compliance (“Form I-9”) is providing this notice of a cybersecurity event to your office on behalf of itself and its customers listed in Exhibit A. Form I-9 assists its customers in completing government required Form I-9 documents. In the course of providing these services, Form I-9 collects personal information associated with its customers’ employees for the purpose of completing these forms.

On April 12, 2024, Form I-9 discovered that an unauthorized third party obtained access to a portion of Form I-9’s network, including the legacy Form I-9 application. Upon becoming aware of this unauthorized access, Form I-9 promptly took steps to protect the integrity of its systems and data, including by taking portions of its network offline, launching an investigation with the assistance of external cybersecurity experts, and notifying law enforcement. Form I-9’s investigation has determined that the unauthorized third party gained access to the Form I-9 network on or about February 5, 2024 using a compromised account associated with Form I-9’s third-party managed IT service provider.

As of May 6, 2024, we determined that approximately 120 Maryland residents were affected. Depending on the individual, the types of affected data may have included: first name, last name, address, Social Security number, date of birth, and hire date. Form I-9’s monitoring has not revealed any indication that this personal information has been leaked or otherwise misused for fraud or identity theft purposes. Form I-9’s investigation and review of the affected data is ongoing, and we anticipate additional rounds of notifications associated with this event.

Form I-9 began sending formal notification to the affected individuals via U.S. mail on May 31, 2024. Attached is a copy of the consumer notification mailed to the affected individuals in your state. Form I-9 is providing affected individuals with 24 months of complimentary credit monitoring and identity theft protection services through Experian. We have also established a dedicated call center to answer individuals’ questions.

We have also taken, and will continue to take, proactive measures to protect our systems and data, including enhancing access controls and security protocols, and implementing additional monitoring technologies and procedures. Specifically, upon discovering the incident, Form I-9 promptly took the affected portions of its network offline and reset all customer credentials relating to the affected

legacy Form I-9 application. Form I-9 has since fully disabled the legacy application and fully rebuilt the application in a more secure Azure-hosted tenant. Form I-9 has also implemented multifactor authentication on all employee accounts and decommissioned the affected corporate network.

If you have any questions, please contact me at thomas.brechtel@fadv.com.

Regards,

Thomas Brechtel

Form I-9 Compliance

Exhibit A

Aimbridge Hospitality

Dycom Industries, Inc.



<<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 / Security Incident])>>

Dear <<first_name>>:

We are writing to let you know of a cybersecurity incident that we, Form I-9 Compliance (“Form I-9”), recently experienced. As you may be aware, our service assists our customers in completing the government required Form I-9 documents in connection with your employment. In the course of our relationship with <<b2b_text_2 (Customer Name)>>, Form I-9 was provided certain of your information in order to complete the form and this information was affected by this incident.

We are providing you with information about the incident, our response, and additional measures you can take to help protect yourself. Importantly, we are not aware of fraud or misuse of your personal information resulting from this incident.

What Happened?

On or about February 5, 2024, an unauthorized third party obtained access to a portion of Form I-9’s network. On April 12, 2024, we became aware of the unauthorized activity and promptly took a portion of our network offline, activated our response process, and launched an investigation of the incident with the support of external cybersecurity experts. We also reported the incident to law enforcement.

What Information Was Involved?

Our investigation determined that some of your personal information was affected by this incident. This information included your <<b2b_text_3 (Data Elements)>>.

What We Are Doing.

As part of our response, we have worked with external cybersecurity experts to confirm the unauthorized third party no longer has access to our company systems. We have also reset all account credentials associated with the affected portion of our network, and we have implemented additional security measures with the guidance of external experts to strengthen the ongoing security of our network.

While we are not aware of identity theft or fraud related to information affected by this incident, as an additional precaution, we are offering you two years of complimentary credit monitoring and identity restoration services through Experian. Details about this offer and instructions on how to activate these services are enclosed with this letter. You must enroll by <<b2b_text_6 (Activation Deadline)>> to use these services.

What You Can Do.

We encourage you to remain vigilant and review your account statements and free credit reports regularly to ensure there is no unauthorized or unexplained activity. We also encourage you to enroll in the complimentary credit monitoring services that we are offering. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains details about this offer and general guidance on what you can do to safeguard against possible future misuse of your information.

For More Information.

Form I-9 has established a dedicated call center to answer questions about this incident. If you have any questions regarding this incident, please call <<insert call center >> Monday through Friday 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Form I-9 Customer Support

Form I-9 Compliance

Steps You Can Take to Help Protect Personal Information

Enroll in Experian's Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

We encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- **Enroll by 5:59pm CT on <<b2b_text_6 (Activation Deadline)>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: <<activation code s_n>>**

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to Experian. If, after discussing your situation with an Experian agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is immediately available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

If you have questions about the product, need assistance with Identity Restoration as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by August 30, 2024. Be prepared to provide engagement number <<b2b_text_4 Engagement Number>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

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

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the

victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the three major credit reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

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

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, under Massachusetts law, individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair

Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. [There are approximately \[#\] Rhode Island residents that may be impacted by this event.](#)



October 11, 2024

BY EMAIL

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

To Whom It May Concern:

Form I-9 Compliance (“Form I-9”) is providing this supplemental notice of a cybersecurity event to your office on its own behalf and on behalf of its customers listed in Exhibit A. Form I-9 assists its customers in completing government required Form I-9 documents. In the course of providing these services, Form I-9 collects personal information associated with its customers’ employees for the purpose of completing these forms.

On April 12, 2024, Form I-9 discovered that an unauthorized third party obtained access to a portion of Form I-9’s network, including the legacy Form I-9 application. Upon becoming aware of this unauthorized access, Form I-9 promptly took steps to protect the integrity of its systems and data, including by taking portions of its network offline, launching an investigation with the assistance of external cybersecurity experts, and notifying law enforcement. Form I-9’s investigation has determined that the unauthorized third party gained access to the Form I-9 network on or about February 5, 2024, using a compromised account associated with Form I-9’s third-party managed IT service provider, and leveraged this access to remove certain documents containing personal information from the network.

Upon gaining access to the affected documents, Form I-9 undertook an extensive review to determine the number of individuals and types of data affected. In order to notify affected individuals as promptly as possible, Form I-9 began sending formal individual notifications on behalf of its customers via U.S. mail on May 31, 2024, and has continued to notify affected individuals on a rolling basis as they have been identified. Form I-9 completed its review of the affected data on September 10, 2024, and began notifying the affected data owners of this incident on September 27, 2024.

At this time, we have determined that a total of approximately 470 Maryland residents were affected. Depending on the individual, the types of affected data may have included: first name, last name, date of birth, Social Security number, driver's license number, other government issued ID, signature, alien registration number, and passport number. Form I-9’s monitoring has not revealed any indication that this personal information has been leaked or otherwise misused for fraud or identity theft purposes.

Attached is a copy of the consumer notification mailed to the affected individuals in your state. Form I-9 is providing affected individuals with 24 months of complimentary credit monitoring and identity theft protection services through Experian. We have also established a dedicated call center

to answer individuals' questions. Form I-9's notifications are substantially complete at this time. We do not expect any significant changes in our notifications and therefore do not anticipate providing further updates unless requested by your office.

We have also taken, and will continue to take, proactive measures to protect our systems and data, including enhancing access controls and security protocols, and implementing additional monitoring technologies and procedures. Specifically, upon discovering the incident, Form I-9 promptly took the affected portions of its network offline and reset all customer credentials relating to the affected legacy Form I-9 application. Form I-9 has since fully disabled the legacy application and fully rebuilt the application in a more secure Azure-hosted tenant. Form I-9 has also implemented multifactor authentication on all employee accounts and decommissioned the affected corporate network.

If you have any questions, please contact me at thomas.brechtel@fadv.com.

Regards,

Thomas Brechtel

Form I-9 Compliance

Exhibit A

Form I-9 Compliance (“Form I-9”) is providing this notice of a cybersecurity event to your office on its own behalf and on behalf of its customers listed below.

Data Owner	Number of Affected Residents Per Data Owner
Teletech Corp.	255
Aimbridge Hospitality	123
ISS Facility Services Inc.	44
Waste Management	21
Arrow Electronics, Inc.	6
Anywhere Real Estate Inc.	4
Fallon Health	4
Coolsys Commercial & Industrial Solutions Inc.	2
Employbridge	1
InfraServices Group Wireless LLC	1



<<Date>>

<<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>> <<State>> <<Zip Code>>

<<Variable Text 1 (Notice of /Data Breach / Security Incident)>>

Dear <<First Name>>:

We are writing to let you know of a cybersecurity incident that occurred at Form I-9 Compliance (“Form I-9”) that affected some of your personal information. As you may be aware, our services assist our customers in completing government required Form I-9 documents.

We are providing you with information about the incident, our response, and additional measures you can take to help protect yourself. Importantly, we are not aware of fraud or misuse of your personal information resulting from this incident.

What Happened?

On or about February 5, 2024, an unauthorized third party obtained access to a portion of Form I-9’s network. On April 12, 2024, we became aware of the unauthorized activity and promptly took a portion of our network offline, activated our response process, and launched an investigation of the incident with the support of external cybersecurity experts. We also reported the incident to law enforcement.

What Information Was Involved?

Our investigation determined that some of your personal information was affected by this incident. This information included your name, address, <<Variable Text 2 (Data Elements)>>.

What We Are Doing.

As part of our response, we have worked with external cybersecurity experts to confirm the unauthorized third party no longer has access to our company systems. We have also reset all account credentials associated with the affected portion of our network, and we have implemented additional security measures with the guidance of external experts to strengthen the ongoing security of our network.

While we are not aware of identity theft or fraud related to information affected by this incident, as an additional precaution, we are offering you two years of complimentary credit monitoring and identity restoration services through Experian. Details about this offer and instructions on how to activate these services are enclosed with this letter. You must enroll by <<Variable Text 3 (Activation Deadline)>> to use these services.

What You Can Do.

We encourage you to remain vigilant and review your account statements and free credit reports regularly to ensure there is no unauthorized or unexplained activity. We also encourage you to enroll in the complimentary credit monitoring services that we are offering. Please review the enclosed Steps

You Can Take to Help Protect Personal Information, which contains details about this offer and general guidance on what you can do to safeguard against possible future misuse of your information.

For More Information.

Form I-9 has established a dedicated call center to answer questions about this incident. If you have any questions regarding this incident, please call (866) 898-2270, Monday through Friday 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Form I-9 Customer Support

Form I-9 Compliance

Steps You Can Take to Help Protect Personal Information

Enroll in Experian's Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

We encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- **Enroll by 5:59pm CT on** <<Variable Text 3 (Activation Deadline)>> (Your code will not work after this date).
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: <<Variable 4 (Activation Code)>>

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to Experian. If, after discussing your situation with an Experian agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is immediately available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

If you have questions about the product, need assistance with Identity Restoration as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-918-1117 by January 31, 2025. Be prepared to provide engagement number **B132474** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.

- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

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

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/credit-freeze	https://www.experian.com/freeze/center.html	https://www.transunion.com/credit-freeze
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the three major credit reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

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

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, under Massachusetts law, individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and <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 Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at www.dfcs.oregon.gov/id_theft.html and click “How to get a security freeze.”

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event.



November 7, 2024

BY EMAIL

**Maryland Attorney General
200 St. Paul Place
Baltimore, Maryland
idtheft@oag.state.md.us**

To Whom It May Concern,

Form I-9 Compliance (“Form I-9”) initially notified your office May 31, 2024 of a cybersecurity incident that Form I-9 discovered on April 12, 2024. We provided your office with an update on the status of Form I-9’s investigation and notifications on October 11, 2024. Form I-9 is making this final notification on its own behalf and on behalf of its customers listed in **Exhibit A**.

Form I-9’s notifications are substantially complete at this time. Although we are in the process of attempting to identify address information for a small set of affected individuals, we do not expect any significant changes in our notifications and therefore do not anticipate providing further updates unless requested by your office.

As you are aware, upon gaining access to the affected documents, Form I-9 undertook an extensive review to determine the number of individuals and types of data affected. Form I-9 began sending formal individual notifications on behalf of its customers via U.S. mail on May 31, 2024, and has continued to notify affected individuals on a rolling basis as they have been identified. As of November 7, 2024 Form I-9 will have notified 2,630 Maryland residents of this incident. Depending on the individual, the types of affected data may have included: first name, last name, date of birth, Social Security number, tax ID number, driver's license number, other government issued ID, signature, alien registration number, fingerprint scan, passport number, state issued ID number, and treatment information, diagnosis or prescription information.

Form I-9 is providing affected individuals with 24 months of complimentary credit monitoring and identity theft protection services through Experian and has established a dedicated call center to answer customer questions. Form I-9’s monitoring has not revealed any indication that the affected information has been leaked or otherwise misused for fraud or identity theft purposes.

If you have any questions, please contact me at thomas.brechtel@fadv.com.

Regards,

Thomas Brechtel

Form I-9 Compliance

Exhibit A

Form I-9 Compliance (“Form I-9”) is providing this notice of a cybersecurity event to your office on its own behalf and on behalf of its customers listed below.

Data Owner	Number of Affected Residents Per Data Owner
Dycom Industries, Inc.	1811
Teletech Corp.	268
Sprouts Farmers Market, Inc.	122
University Of Toledo	68
ADT Solar	48
ISS Facility Services, Inc.	45
Waste Management	21
MSL Corporate	20
Capital Group	15
TPUSA, Inc.	15
Black & Veatch Construction, Inc.	8
Arrow Electronics, Inc.	7
Fallon Health	4
Pearce Services, Inc.	4
Anywhere Real Estate Inc.	4
STC Netcom, Inc.	3
Sutter Health	3
Tower Communications Expert LLC	3
Advanced Communications Technology LLC	2
Coolsys Commercial & Industrial Solutions, Inc.	2

Henkels & McCoy Group, Inc.	2
AMP Communications LLC	1
Apex Site Solutions, Inc.	1
California Utility Company	1
Calsoft Labs Inc	1
Corby Energy Services Inc	1
Costich Engineering D.P.C.	1
Davey Tree Expert Company	1
DLSI	1
Dun & Bradstreet	1
Earthcom, Inc.	1
EBI Consulting, Inc.	1
EFI Engineering	1
Employbridge	1
Ethos Distributed Solutions, Inc.	1
Fullerton Engineering Consultants, Inc.	1
Greentech Services LLC	1
Gulf Equipment Corp D/B/A Gulf Services	1
H&R Paving, Inc.	1
Harris	1
InfraServices Group Wireless LLC	1
Inland Valley Construction	1
Intellicom Communications, Inc.	1

J Crompton Electric, Inc.	1
Joy Inc.	1
Mason Wireless Solutions Ltd.	1
Medical Solutions LLC	1
NXT Telcom Services, Inc.	1
RoadSafe Traffic Systems, Inc .	1
Stripe It Up	1
The Barricade Company LLC	1
United Staffing	1
Vision Telecommunications, Inc.	1