



Colin D. Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

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

August 27, 2024

VIA E-MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent Legacy Capital Advisors LLC (“Legacy”) located at 4401 North Side Parkway Northwest, Suite 900, Atlanta, Georgia 30327, and are writing to notify your office of an incident that may affect the security of certain personal information relating to ten (10) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Legacy does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about September 25, 2023, Legacy discovered suspicious activity related to an employee’s email account. In response, Legacy immediately took steps to secure the affected account and initiated an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined that an unauthorized actor gained access to several employee email accounts beginning in late July 2023, and subsequently had access to the data contained therein. Therefore, Legacy conducted a comprehensive review of the contents of the accounts to identify the type of information present and to whom the information relates. Legacy completed the review on March 20, 2024, and confirmed that sensitive information related to some individuals was contained therein. Legacy then worked to locate accurate address information for the impacted individuals. The information that could have been subject to unauthorized access includes: name, Social Security number, and driver’s license number.

Notice to Maryland Residents

On August 26, 2024, Legacy began mailing written notice of this incident to potentially affected individuals for whom it had a postal address which included ten (10) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit A**. Legacy also posted notice of the event on the homepage of its website (<https://www.yourlegacyteam.com/>) and published a media notice throughout the state of Georgia regarding the event on August 27, 2024. Attached is a copy of the website notice as **Exhibit B** and the media notice as **Exhibit C**.

Other Steps Taken and To Be Taken

Upon discovering the event, Legacy moved quickly to investigate, assess the security of the impacted accounts, and identify potentially affected individuals. Further, Legacy notified federal law enforcement of the event. Legacy also implemented additional safeguards to help prevent similar incidents from occurring in the future. Legacy is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one (1) year through Experian at no cost to the individuals.

Additionally, Legacy is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Legacy is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Legacy is providing written notice of this incident to state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4259.

Very truly yours,



Colin D. Scanlon of
MULLEN COUGHLIN LLC

EXHIBIT A

LEGACY CAPITAL ADVISORS LLC

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 26, 2024

L8924-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Notice of [Variable Text 1]

Dear Sample A. Sample:

Legacy Capital Advisors LLC (“Legacy” or “We”) writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your information should you feel it appropriate to do so.

What Happened? On September 25, 2023, Legacy discovered suspicious activity related to an employee’s email account. In response, we immediately took steps to secure the affected account and initiated an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined that an unauthorized actor gained access to several employee email accounts beginning in late July 2023, and subsequently had access to the data contained therein. Therefore, Legacy conducted a comprehensive review of the contents of the accounts to identify the type of information present and to whom the information relates. On March 20, 2024, we completed this extensive review and identified that information pertaining to certain individuals was present in the affected accounts, we then worked to locate accurate address information for the impacted individuals.

What Information Was Involved? The following information related to you was contained in one of the impacted accounts: [variable text 2]. Although our investigation was unable to confirm whether your information was actually viewed by the unauthorized actor, we are unable to rule out the possibility.

What We Are Doing. The confidentiality, privacy, and security of information is among our highest priorities. Upon becoming aware of this incident, we took steps to secure the impacted email accounts and performed a full investigation. We also implemented additional security measures to protect against similar incidents moving forward.

As an added precaution, we are offering you access to complimentary credit monitoring and identity theft protection services for [variable text 3] months through Experian. The deadline to enroll in these services is November 29, 2024. Please note that you will not be automatically enrolled in these services, so should you wish to enroll you will need to do so on your own. You can find instructions on how to enroll in these services in the enclosed *Steps You Can Take to Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Protect Personal Information* for additional guidance.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions, you can call our dedicated assistance line at 1-833-918-3955 which is available Monday through Friday, between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time, excluding major U.S. holidays. You can also write to us at 4401 Northside Parkway Northwest, Suite 900, Atlanta, Georgia 30327.

We sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

The Legacy Team



STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

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

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 an Experian agent. If, after discussing your situation with an 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 available to you for ## 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-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:

- Ensure that you **enroll by** November 29, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose 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 1-833-918-3955 by November 29, 2024. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-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 ExtendCARETM:** 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, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

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

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

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

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

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. 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; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.



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

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

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

EXHIBIT B



Notice of Data Security Event



August 27, 2024 – Legacy Capital Advisors (“Legacy”) recently discovered an incident that may have impacted the privacy of information related to certain individuals. This notice provides details of the incident, Legacy’s response, and steps individuals may take to help protect their personal information should they feel it is appropriate to do so.

What Happened? On September 25, 2023, Legacy discovered suspicious activity related to an employee’s email account. In response, we took steps to secure the affected account and initiated an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined that an unauthorized actor gained access to several employee email accounts beginning in late July 2023, and subsequently had access to the data contained therein. Therefore, Legacy conducted a comprehensive review of the contents of the accounts to identify the type of information present and to whom the information relates. On March 20, 2024, we completed this extensive review and identified that information pertaining to certain individuals was present in the affected accounts, we then worked to locate accurate address information for the impacted individuals.

What Information Was Involved? While the specific data potentially at risk varies for each individual, the scope of information involved may include an individual’s name, Social Security number, taxpayer identification number, driver’s license number, electronic/digital signature, username and password, date of birth, medical information, payment card information, health insurance information, financial account information, passport number, and employer identification number.

How Will Individuals Know If They Are Affected By This Incident? Legacy is mailing notice letters to potentially affected individuals for whom it has a mailing address. Individuals who do not receive a letter but think they may be impacted, may call the dedicated assistance line listed below to inquire further.

What We Are Doing. The confidentiality, privacy, and security of information is among our highest priorities. Upon becoming aware of this incident, we took steps to secure the impacted email accounts and performed a full investigation. We also implemented additional security measures to protect against similar incidents moving forward.

What You Can Do. Legacy encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the information contained in the below *Steps You Can Take to Protect Personal Information* for additional guidance.

Whom Should Individuals Contact for More Information? If you have questions, you can call our dedicated assistance line at 1-833-918-3955 which is available Monday through Friday between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time, excluding major U.S. holidays.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.



alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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



For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; 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 www.oag.state.md.us.

For Massachusetts Residents, Under Massachusetts law, you 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, 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, DC 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.



Office: (404) 267-1358

4401 Northside Parkway North West
Suite 900
Atlanta, GA 30327

info@yourlegacyteam.com

Quick Links

[Retirement](#)

[Investment](#)

[Estate](#)

[Insurance](#)

[Tax](#)

[Money](#)

[Lifestyle](#)

[All Articles](#)

[All Videos](#)

[All Calculators](#)

Check the background of your financial professional on FINRA's [BrokerCheck](#).

The content is developed from sources believed to be providing accurate information. The information in this material is not intended as tax or legal advice. Please consult legal or tax professionals for specific information regarding your individual situation. Some of this material was developed and produced by FMG Suite to provide information on a topic that may be of interest. FMG Suite is not affiliated with the named representative, broker - dealer, state - or SEC - registered investment advisory firm. The opinions expressed and material provided are for general information, and should not be considered a solicitation for the purchase or sale of any security.

We take protecting your data and privacy very seriously. As of January 1, 2020 the [California Consumer Privacy Act \(CCPA\)](#) suggests the following link as an extra measure to safeguard your data: [Do not sell my personal information](#).

Copyright 2024 FMG Suite.

Securities offered through Avantax Investment ServicesSM, Member [FINRA](#), [SIPC](#). Investment advisory services offered through Avantax Advisory ServicesSM. Insurance services offered through an Avantax affiliated insurance agency.

The information contained in this e-mail message is being transmitted to and is intended for the use of only the individual(s) to whom it is addressed. If the reader of this message is not the intended recipient, you are



EXHIBIT C

MEDIA STATEMENT

For Immediate Release:

Legacy Capital Advisors LLC Provides Notice of a Data Security Event

Legacy Capital Advisors LLC (“Legacy”) discovered an incident that may have impacted the privacy of information related to certain individuals. This notice provides details of the incident, Legacy’s response, and steps individuals may take to help protect their personal information should they feel it is appropriate to do so.

On or about September 25, 2023, Legacy discovered suspicious activity related to an employee’s email account. In response, Legacy took steps to secure the affected account and initiated an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined that an unauthorized actor gained access to several employee email accounts beginning in late July 2023, and subsequently had access to the data contained therein. Therefore, Legacy conducted a comprehensive review of the contents of the accounts to identify the type of information present and to whom the information relates. Legacy is mailing notice letters to potentially affected individuals for whom it has a mailing address.

While the specific data potentially at risk varies for each individual, the scope of information involved may include an individual’s name, Social Security number, taxpayer identification number, driver’s license number, electronic/digital signature, username and password, date of birth, medical information, payment card information, health insurance information, financial account information, passport number, and employer identification number.

The confidentiality, privacy, and security of information in Legacy’s care is among its highest priorities. Legacy encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity.

Interested individuals can find additional information about the event and how they can help protect their personal information at <https://www.yourlegacyteam.com/>. They may also write to Legacy at 4401 Northside Parkway Northwest, Suite 900, Atlanta, Georgia 30327.