



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

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

January 16, 2025

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 Southwest Stage Funding, LLC d/b/a Cascade Financial Services (“Cascade”) located at 2290 E. Yeager Drive, Suite 250, Chandler, AZ 85286 and are writing to notify your office of an incident that may affect the security of certain personal information relating to seven (7) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Cascade 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 July 9, 2024, Cascade became aware of suspicious activity related to certain employee email accounts. Cascade promptly took steps to secure the email tenant and initiated an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. The investigation determined that between July 8, 2024 and July 9, 2024, certain email accounts were accessed and downloaded by an unknown actor. As such, Cascade engaged a data review vendor to conduct a comprehensive and time-intensive review of the contents of the affected email accounts to identify any personal information contained therein and to whom that information relates. After Cascade received the results of this extensive review process from the data review vendor, Cascade engaged in additional work to review and verify the affected information and locate address information for the potentially impacted population. Cascade completed this analysis on December 31, 2024, and worked to issue notifications as expeditiously as possible.

The potentially impacted information varies per individual and may include name, Social Security number, and driver’s license number.

Notice to Maryland Residents

On January 16, 2025, Cascade provided written notice of this incident to seven (7) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Cascade moved quickly to investigate and respond to the incident, assess the security of Cascade's email environment, and identify potentially affected individuals. Cascade is working to implement additional safeguards and training to its employees. Cascade is providing access to credit monitoring services for one (1) year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Cascade 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. Cascade is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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.

Cascade is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,

Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/ogf
Enclosure

EXHIBIT A



<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<Date>>

NOTICE OF [SECURITY INCIDENT] / [DATA BREACH]

Dear <<Name 1>> <<Name 2>>:

Southwest Stage Funding, LLC d/b/a Cascade Financial Services (or, in Delaware, Oregon, Pennsylvania, and Washington, Cascade Land-Home Financing) ("Cascade") writes to inform you of an event that may affect the privacy of some of your personal information. Although we are unaware of any identity theft or fraud in relation to the event, we are providing you with information about the event, our response, and resources we are making available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On July 9, 2024, we became aware of suspicious activity related to certain employee email accounts. We promptly took steps to secure the email tenant and initiated an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. The investigation determined that between July 8, 2024 and July 9, 2024, certain email accounts were accessed and downloaded by an unknown actor. As such, we engaged a data review vendor to conduct a comprehensive and time-intensive review of the contents of the affected email accounts to identify any personal information contained therein and to whom that information relates. After we received the results of this extensive review process from the data review vendor, we engaged in additional work to review and verify the affected information and locate address information for the potentially impacted population. We completed this analysis on December 31, 2024, and confirmed that certain information related to you was contained within the affected email accounts.

What Information Was Involved? The review determined the following types of information related to you were present in the affected email accounts: your [data elements]. While we are unaware of any actual or attempted misuse of your information as a result of this event, we are notifying you out of an abundance of caution.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care are among our highest priorities. Upon becoming aware of this event, we secured the email tenant, investigated what happened, and reviewed the contents of the impacted email accounts to identify any individuals that may have been affected. As part of our ongoing commitment to the privacy of information in our care, we are implementing additional security measures to further protect against similar events occurring in the future.

As an added precaution, we are offering you credit monitoring and identity theft protection services for [12/24] months through IDX at no cost to you. Please note that you will not be automatically enrolled in these services. We encourage you to enroll in these services as we are not able to do so on your behalf. You can find information on how to enroll in these services in the enclosed *STEPS YOU CAN TAKE TO HELP 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 free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. You may also enroll in the complimentary credit monitoring and identity theft protection services we are offering. Please also review the information contained in the enclosed *STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION*.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions or need assistance, please call [(###) ###-####] from [X:00 a.m. - X:00 p.m.], Eastern

Time, Monday through Friday, excluding major U.S. holidays. You may also write to us at 2290 E. Yeager Drive, Suite 250, Chandler, AZ 85286.

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

Sincerely,

Southwest Stage Funding, LLC
d/b/a Cascade Financial Services
or Cascade Land-Home Financing

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Restoration

[Enrollment Instructions]

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 you 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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; 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 are approximately [#] Rhode Island residents that may be impacted by this event.